Problematika digitálních stop a jejich zajišťování na místě činu

Bc. Jakub Synek

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jakub Synek**
Osobní číslo:	**A15234**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Problematika digitálních stop a jejich zajišťování na místě činu**
Téma anglicky:	**The Problems and Issues of Digital Evidence and its (Subsequent) Securing on a Crime Scene**

Zásady pro vypracování:

1. **Objasněte problematiku digitálních důkazů.**
2. **Specifikujte vhodné metody pro zajišťování digitálních stop na místě činu.**
3. **Popište možné způsoby vytváření bitových kopií a záloh digitálních stop.**
4. **Zhodnoťte rizika práce s digitálními stopami.**
5. **Porovnejte a vyhodnoťte jednotlivé metody pro zajišťování digitálních stop na místě činu.**
6. **Navrhněte jednotný technologický postup pro zajišťování digitálních stop na místě činu z hlediska jeho efektivity a následné vytěžitelnosti získaných dat.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.**
2. **PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-589-0.**
3. **KONRÁD, Zdeněk a Jiří STRAUS. Kriminalistika: teorie, metodologie a metody kriminalistické techniky. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. ISBN 978-80-7380-535-7.**
4. **PORADA, Viktor. Kriminalistika: (teorie, metody, metodologie). Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. ISBN 978-80-7380-490-9.**
5. **KOTHÁNEK, Jaroslav. Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení. Praha: Policie ČR, 2008.**
6. **CASEY, Eoghan. Digital evidence and computer crime: forensic science, computers and the Internet. 3rd ed. Waltham, MA: Academic Press, c2011. ISBN 0123742684.**
7. **NELSON, Bill. Guide to computer forensics and investigations: processing digital evidence. Fifth edition. Boston, MA: Cengage learning, 2016. ISBN 9781285060033.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **24. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 19. 5. 2017 …….

podpis diplomanta

ABSTRAKT

Diplomová práce objasňuje problematiku výskytu digitálních stop na místě činu a uvádí možné postupy využitelné pro jejich zajišťování v rámci provádění úkonů trestního řízení. Teoretická část práce je věnována obecné charakteristice digitálních stop, jsou zde definovány jejich vlastnosti a zákonitosti a dále je v této části práce věnována pozornost legislativním aspektům, které jsou v rámci zajišťování stop uplatňovány. V praktické části práce je provedeno stanovení a hodnocení rizik, která souvisí s prací s digitálními stopami a následně jsou formulovány metody, které jsou vhodné pro zajišťování digitálních stop. Na základě hodnocení jednotlivých rizik a metod práce s digitálními stopami je navržen optimální technologický postup ve vztahu k zajišťování digitálních stop na místě činu tak, aby došlo k jejich úplnému zajištění a zároveň byla minimalizována veškerá hrozící rizika.

Klíčová slova: digitální stopa, vyšetřování, kyberkriminalita, policie, forenzní postupy, trestná činnost, důkazní materiál, počítačová technika, mobilní zařízení, hash

ABSTRACT

This diploma thesis clarifies the issue of the occurrence of digital evidence at the crime scene and outlines the possible procedures that can be used to provide them in the course of the criminal proceedings. The theoretical part is devoted to the general characteristics of digital tracks, their properties and patterns. In this part of the diploma thesis is paid attention to the legislative aspects that are applied in the provision of digital evidence. In the practical part of this thesis, the assessment and evaluation of the risks associated with the work with digital tracks is carried out and then the methods that are suitable for providing traces are formulated. Based on individual risk assessments and digital tracking methods, an optimal technological approach is proposed in relation to the provision of digital evidence at the crime scene so that they are fully secured and at the same time minimizing all imminent risks.

Keywords: Digital evidence, investigation, cybercrime, police, forensic procedures, criminal activity, evidence, computer technology, mobile devices , hash

Děkuji svému vedoucímu Ing. Davidu Malaníkovi, Ph.D. za cenné rady, ochotu a vstřícnost, které se mi dostávalo v průběhu psaní této práce. Poděkování patří i mé manželce Kateřině a celé rodině za toleranci, pochopení a podporu při studiu.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Práce s výpočetní a komunikační technikou se stala za posledních několik let nedílnou a neodmyslitelnou součástí našeho života. Počítače, telefony a různá jiná záznamová zařízení používáme téměř denně. Do svých mobilních telefonů, notebooků a přenosných USB disků ukládáme stále více dat nejen pracovního, ale i soukromého charakteru. A právě z tohoto důvodu jsou naše elektronická zařízení tak cenným artiklem na poli získávání digitálních důkazů. Prakticky každé elektronické zařízení, které se nachází na místě kriminalisticky relevantní události, je pro potřeby vyšetřování digitální stopou, která může ve svém obsahu ukrývat cenné důkazní materiály.

V rámci této diplomové práce je věnována pozornost procesu zajišťování digitálních stop na místě, kde dochází k provádění úkonů v rámci trestního řízení. Úvodní kapitola je věnována charakteristice digitálních stop a jejich významu pro objasňování trestní věci. Pojímá tak problematiku digitálních stop ve vztahu k zákonitostem, kterým digitální stopy podléhají, a které na stopy působí. Dostatečný prostor je věnován i objasnění právních aspektů, tedy toho, za jakých okolností mohou být digitální stopy zajišťovány a v jakých případech jsou v rámci trestního řízení upotřebitelné. Teoretická část práce dále pojednává o jednotlivých typech digitálních stop, které se mohou na místě realizace úkonů v rámci trestního řízení vyskytovat, a definuje jednotlivé metody a postupy, které jsou v procesu zajišťování digitálních stop upotřebitelné.

Praktická část práce si klade za cíl zmapovat postup jednotlivých činností, které jsou v rámci zajišťování digitálních stop prováděny, a na jejich základě definovat, jaká rizika mohou v jednotlivých fázích zajišťování stop hrozit, a vést tak k poškození nebo znehodnocení zajištěné digitální stopy. Dále je v praktické části provedeno zmapování jednotlivých postupů a metod, které jsou používány v rámci zajišťování digitálních stop na místě činu a na základě předešlého hodnocení rizik je navržen optimální postup pro zajišťování digitálních stop tak, aby byla hrozící rizika v průběhu zajišťování stop minimalizována.

Tato práce má poukázat na zvyšující se frekvenci výskytu digitálních stop na místě činu, na jejich rostoucí se význam pro objasňování trestní věci, ale také na složitost a komplexnost celé problematiky.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY DIGITÁLNÍCH STOP

Rostoucí tendence výskytu digitálních stop na místě vzniku kriminalisticky relevantní události zvyšuje význam využitelnosti digitálních důkazů pro objasňování trestní věci. Digitální stopy se v současné době nacházejí prakticky všude kolem nás. Mají své zákonitosti, svá specifika, ale také svá úskalí.

1.1 Legislativa ve vztahu k digitálním stopám

Samotný proces zajištění digitálních stop je jedním z nejdůležitějších úkonů pro úspěšné vyšetřování počítačové kriminality, nebo jiné trestné činnosti, k jejímuž páchání byla použita počítačová a komunikační technika, nebo v této technice mohou být obsaženy informace, které jsou zásadní pro prokázání dané trestné činnosti. Celý proces zajišťování digitálních stop však musí probíhat za předpokladu, že tyto stopy budou před soudem akceptovány jako důkaz. Při samotném zajišťování digitálních stop tedy musí být dodržena stránka legality tak, jako je tomu u zajišťování ostatních důkazních materiálů (listinných dokumentů, předmětů, zbraní, apod.). [10]

Digitální stopy jsou proto v rámci objasňování trestní věci zajišťovány na základě soudního rozhodnutí, a jejich zajišťování tak provádí orgány činné v trestním řízení zejména prováděním těchto úkonů:

- domovní prohlídka,
- prohlídka jiných prostor a pozemků,
- osobní prohlídka,
- vydání věci,
- odnětí věci,
- ohledání místa činu,
- zajištění dat ze sítě Internet,
- a dalšími úkony.

Získávání a zajišťování digitálních stop je ve většině případů prováděno současně s ohledáním místa činu, jehož právní úprava je zakotvena v zákoně č. 141/1961 Sb. o trestním řízení soudním. Dle tohoto zákona se řídí také samotné zajišťování digitálních stop, které lze provádět pouze v případě, kdy je to trestním řádem umožněno. Nejčastěji jsou digitální stopy zajišťovány v rámci provádění domovní prohlídky, osobní prohlídky a prohlídky jiných prostor a pozemků, která je definována v § 82 trestního řádu.

Digitální stopy mohou být dále zajištěny tzv. dobrovolným vydáním věci dle § 78 trestního řádu, nebo v krajním případě lze využít institutu odnětí věci dle § 79 trestního řádu. [2]

1.1.1 Domovní prohlídka, osobní prohlídka a prohlídka jiných prostor a pozemků

Jak bylo uvedeno výše, provedení domovní prohlídky, osobní prohlídky a prohlídky jiných prostor a pozemků je řízeno ustanovením § 82 zákona č. 141/1961 o trestním řízení soudním (trestní řád). Jak je definováno v zákoně, je možné domovní prohlídku, osobní prohlídku a prohlídku jiných prostor a pozemků vykonat pouze za předpokladu, že se v bytě nebo v jiných prostorách určených k bydlení či v prostorách k nim náležející nachází věc nebo osoba, která je důležitá pro trestní řízení. Ze stejného důvodu je možné provést i prohlídku jiných prostor (nesloužících k bydlení) a pozemků. V případě osobní prohlídky je možno tuto provést za předpokladu, je-li důvodné podezření, že má někdo u sebe věc důležitou pro trestní řízení.

Domovní prohlídka je prováděna pouze na základě vydání písemného příkazu k domovní prohlídce, který je vydán předsedou senátu dle ustanovení § 83 trestního řádu, případně je možno domovní prohlídku provést též v přípravném řízení. Zde je vydán příkaz k domovní prohlídce na návrh státního zástupce soudcem. Domovní prohlídku je oprávněn vykonat policejní orgán.

Stejně tak provedení prohlídky jiných prostor a pozemků je možno provést pouze na základě vydaného příkazu k prohlídce. Ten je vydáván na základě ustanovení § 83a trestního řádu, a k jeho vydání je oprávněn předseda senátu. Bez příkazu lze prohlídku jiných prostor a pozemků provést pouze za předpokladu, že vydání příkazu nelze předem dosáhnout a že věc nesnese odkladu. V takovéto situaci je však policejní orgán povinen si dodatečně souhlas vyžádat, v opačném případě nelze výsledek prohlídky použít jako důkaz v dalším řízení.

Na základě vydaného příkazu k osobní prohlídce dle § 83b trestního řádu vydaného předsedou senátu, případně v přípravném řízení státním zástupcem je prováděna tzv. osobní prohlídka. Tuto lze policejním orgánem vykonat i bez předchozího příkazu, a to za předpokladu, že vydání příkazu nelze dosáhnout a prohlídka nesnese odkladu, nebo pokud se jedná o osobu, která byla přistižena při činu.

Provádění domovní prohlídky, osobní prohlídky, případně prohlídky jiných prostor a pozemků znamená vždy citelný zásah nejen do soukromí, ale převážně i do práv a svobod osob. Z tohoto důvodu je nezbytné před samotnou realizací prohlídky provést předchozí

výslech osob, kterých se připravovaný úkon bude týkat. Tato povinnost je specifikována v § 84 trestního řádu. Pokud v průběhu výslechu dojde k dobrovolnému vydání hledané věci, která je důležitá pro trestní řízení, nelze již domovní prohlídku provést. Pouze v případě, že celá věc nesnese odkladu a hrozí tak nebezpečí z prodlení, není nutné předchozí výslech provádět. Při provádění domovní prohlídky a prohlídky jiných prostor a pozemků musí být vždy přítomna i nezúčastněná osoba a zároveň orgán, který prohlídku provádí, nesmí zapřít účast na prohlídce osobě, u níž je tato prováděna. [2]

1.1.2 Vydání věci a odnětí věci

Znění § 78 trestního řádu hovoří o tom, že kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu, a je-li to nutné pro účely trestního řízení, je povinen takovouto věc orgánům činným v trestním řízení vydat. V případě opačném může být tato věc odňata. Odnětí věci je řízeno dle § 79 trestního řádu, kde se hovoří o tom, že nebude-li věc důležitá pro trestní řízení vydána tím, kdo ji má u sebe, může mu být na příkaz předsedy senátu a v přípravném řízení na příkaz státního zástupce nebo policejního orgánu věc odňata. Tak, jako v případě domovní či osobní prohlídky i zde platí, že jedná-li se o situaci, kdy věc nesnese odkladu a hrozí-li tak nebezpečí z prodlení, lze věc odejmout i bez předchozího souhlasu. K samotnému odnětí věci se přibere i nezúčastněná osoba.

V případě dobrovolného vydání věci dle § 78 trestního řádu pachatel nebo osoba podezřelá spolupracuje. V některých případech se však může stát, že spolupráce ze strany pachatele nebo osoby podezřelé není úplná, a tato osoba se snaží něco zatajit či skrýt a tudíž nevydat věc, která by mohla být pro trestní řízení důležitá. V takovémto případě je doporučeno, aby vyšetřovatel s touto variantou dopředu počítal, a měl také připraven příkaz k domovní prohlídce, který by mohl v případě jakýchkoli pochybností použít a vykonat tak zcela legálně a bez zbytečného odkladu domovní prohlídku či prohlídku jiných prostor a pozemků. [2]

1.1.3 Ohledání místa činu a ohledání věci

Ohledání místa činu a ohledání věci se řadí mezi specifické kriminalisticko-technické metody, kdy je na základě přímého pozorování, zkoumání a hodnocení podchycena materiální situace či stav objektů, které mohou být důležité pro trestní řízení.

Ohledání místa činu má pevně stanovené zásady, kterými jsou:

- neodkladnost,
- neopakovatelnost,
- nezastupitelnost. [8]

Samotný proces ohledání místa činu je právně zakotven v zákoně č. 141/1961 o trestním řízení soudním, konkrétně je upraven v § 158 a § 113 trestního řádu. Zde je také specifikováno, co považujeme za místo činu. Za místo činu považujeme tu část prostoru, kde se uskutečnil proces nebo děj, o kterém je možné podle jeho vnějších projevů předpokládat, že se jedná o děj protispolečenský a u kterého je třeba ohledáním zjistit a zajistit takové znaky jednání, podle nichž by bylo možné věrohodně posoudit, zda jde o trestný čin.

Ohledání místa činu, jak již bylo řečeno, je řazeno mezi tzv. neodkladné úkony, a to hlavně z toho důvodu, že právě místo činu je jediným místem, kde lze bez pochyby najít stopy po činnosti pachatele. Mnohdy se tak jedná prakticky o výchozí bod celého vyšetřování, a vzhledem k jedinečnosti tohoto místa je důležité si zde počínat s maximální opatrností a precizností. Chyby, vzniklé neopatrným postupem na místě činu, se nedají napravit a mohou tak znamenat riziko pro úspěšné vyřešení případu. Ohledání místa činu by mělo pro vyšetřovatele přinést odpověď na sedm základních kriminalistických otázek: CO bylo spácháno?, KDY byl čin spáchán?, KDE byl čin spáchán?, KDO čin spáchal?, JAK byl čin spáchán?, ČÍM byl čin spáchán?, PROČ byl čin spáchán? Je nasnadě uvažovat o tom, že k zodpovězení alespoň jedné otázky může být využito i zajištěním digitálních stop. [1]

1.1.4 Ostatní normy a předpisy vztahující se k problematice digitálních stop

Zajišťování výpočetní a komunikační techniky a dat, které je prováděno Policií České republiky se řadí mezi tzv. kriminalisticko-technické činnosti, které jsou v rámci policie upraveny několika závaznými předpisy. Tyto předpisy neslouží pouze k zachování vysoké odborné úrovně a způsobilosti, ale hovoří také například o tom, kdo a za jakých podmínek je k zajišťování výše zmiňované techniky oprávněn či nikoliv.

Mezi závazné normy, které tuto kriminalisticko- technickou činnost upravují, řadíme:

- Zákon č.36/1967 Sb. o znalcích a tlumočnících,
- Závazný pokyn policejního prezidenta č. 100/2001 ke kriminalisticko-technické činnosti Policie České republiky,

- Závazný pokyn policejního prezidenta č. 77/2009, kterým je upravena věcná, funkční a místní příslušnost znaleckých pracovišť Policie České republiky,
- Pokyn ředitele Kriminalistického ústavu Praha č. 7/2001, kterým je upravena činnost orgánů Policie při zajišťování výpočetní techniky a dat pro účely následného znaleckého zkoumání. [4]

1.2 Charakteristické vlastnosti digitálních stop

Zkoumání dráhy letu střely v balistice nebo zkoumání papilárních linií v daktyloskopii má svá pevně daná pravidla a své zákonitosti. Stejně tak digitální stopy, které nacházíme na místě činu, se řídí svými pravidly a zákonitostmi, které je nutné respektovat a dodržovat, jinak by v opačném případě mohlo dojít k jejich nevratnému poškození nebo porušení jejich integrity.

1.2.1 Nehmotnost digitální stopy

Při práci s digitálními stopami je třeba mít na paměti, že pracujeme se stopami, které jsou velmi citlivé na změnu obsahu a integrity zájmových dat. Jedná se o data, která jsou nehmotná a pokud jsou uložena na pevném disku počítače, či na jiném přepisovatelném záznamovém zařízení, tak jsou tato data velmi lehce pozměnitelná či manipulovatelná. Právě z tohoto důvodu, tedy pro svou nehmotnost, je důležité vždy jakákoliv zájmová data ukládat na nepřepisovatelné médium a pro zajištění kontroly jejich integrity připojit tzv. hash, neboli kontrolní součet (MD5, SHA-1, SHA-2)

1.2.2 Informační hodnota digitální stopy

Digitální stopy jsou v porovnání s ostatními kriminalistickými stopami ve své podstatě jedinečné. Jejich jedinečnost je dána především vysokou informační hodnotou, kterou každá digitální stopa nese. Nejen, že je schopna poskytnout cenné informace o uživateli či pachateli, o jeho zájmech a aktivitách, ale digitální stopa může obsahovat také informace o činnosti uživatele na internetu, o posledních připojených USB zařízeních, nebo o používaných službách a uložených heslech.

1.2.3 Časová trasovatelnost digitální stopy

Obrovským benefitem digitálních stop je jejich tzv. časová trasovatelnost, což je vlastnost prakticky každé digitální stopy, na jejímž základě je možné při provádění forenzní analýzy určit časovou posloupnost jednotlivých dějů, které mohly nastat. Každý digitální dokument,

ať se jedná o psaný text, fotografii, nebo audio záznam si s sebou nese informace o svém původu, čase vytvoření, čase poslední změny, počtu úprav, apod. Všechna digitální zařízení mají informaci o tzv. systémovém čase, což není nic jiného než vnitřní hodiny daného digitálního zařízení, podle kterých jsou jednotlivé aktivity prováděné pomocí aplikačního či systémového vybavení opatřeny tzv. časovou známkou (tzv. timestamp). Za pomoci analýzy těchto časových údajů lze následně určit, kdy proběhlo např. poslední přihlášení k počítači, nebo vytvoření či úprava zájmového dokumentu.

1.2.4 Latentnost digitální stopy

Důležité je se zmínit i o tzv. latentnosti digitálních stop. Jedná se o záznamy, které nejsou pouhým okem viditelné, tzn., že jde o záznamy, které jsou uloženy na některém z datových nosičů, např. pevném disku, CD, nebo BlueRay disku. Dále se v případě latentnosti stop může také hovořit o různých typech systémových záznamů nebo souborů, které nejsou, bez přidělení zvláštních administrátorských práv, pro běžného uživatele viditelné. Za latentní stopy můžeme dále označit i smazané či přepsané soubory na datovém nosiči, zformátované disky, nebo jinak poškozená či pozměněná datová média, k jejichž zpřístupnění je potřeba specializovaný software či vybavení.

1.2.5 Životnost digitální stopy

Digitální stopy mají také svá úskalí, a jedním z nich je jejich nízká životnost. Prakticky všechny digitální záznamy jsou zapisovány na paměťová média, ze kterých mohou být následně cíleně smazány či přepsány jinými záznamy, a to jak samotným uživatelem, nebo systémem. Obnova takto přepsaných dat je samozřejmě možná za použití specializovaného softwaru, ale musí být provedena co nejdříve po smazání či přepsání dat. Zde totiž hraje svou roli počet přepsání smazaných dat. Obecně se dá říci, že čím vícekrát jsou data přepsána, tím je menší šance na jejich obnovení.

1.2.6 Komplexnost digitální stopy

Na celý proces vyšetřování má zásadní vliv, jak kvalitně a včasně jsou stopy zajištěny. Velkou roli zde sehrává tzv. komplexnost prostředí. Zde je třeba rozlišovat, zda se jedná o stopu, kterou lze zajistit jako celek (např. notebook, tablet, mobilní telefon) a nebo, zda přicházíme do styku se stopou, která bude reprezentována například daty, která jsou uložena v rozsáhlém podnikovém informačním systému. V prvním případě, jedná-li se tedy o stopu, kterou lze vyjmout bez porušení její integrity z daného prostředí, je možné tuto stopu odeslat

ke znaleckému zkoumání na znalecké pracoviště. Zajištění takovéto stopy je možné provést bez přítomnosti odborníka z oblasti ICT. V opačném případě, půjde-li o zajištění dat z tzv. živého zkoumaného systému, podnikového informačního systému, nebo bude zapotřebí stahovat zájmová data ze vzdálených cloudových úložišť a firemních serverů, je účast ICT odborníka na tomto úkonu prakticky nezbytná. [10]

2 METODY A POSTUPY ZAJIŠŤOVÁNÍ DIGITÁLNÍCH STOP

Volba metody, která bude zvolena pro zajištění libovolné digitální stopy na místě činu, představuje v rámci správného stanovení technicko-taktického postupu klíčový okamžik, který může zásadním způsobem ovlivnit celkovou situaci nejen na místě, kde probíhají úkony v rámci trestního řízení – tedy na místě domovní prohlídky či prohlídky jiných prostor, ale může také zásadně ovlivnit následnou využitelnost či vytěžitelnost získaných digitálních stop.

2.1 Metody zajišťování digitálních stop na místě činu

Proces samotného zajištění výpočetní a komunikační techniky je z hlediska maximalizace vytěžitelnosti všech digitálních stop naprosto zásadní. Právě z tohoto důvodu by zajišťování techniky měla provádět, či alespoň dozorovat osoba znalce, která bude vystupovat jako garant toho, že všechny stopy budou zajištěny korektně a dle doporučených technologických postupů. V následujících podkapitolách jsou uvedeny nejčastěji se vyskytující příklady metod, které mohou být použity pro zajišťování digitálních stop na místě kriminalisticky relevantní události.

2.1.1 Zajištění stopy „in natura“

Zajištění stopy „in natura“ spočívá v zajištění stopy na místě činu bez toho, aniž by bylo prováděno jakékoliv další zálohování či zkoumání dané stopy. Takováto stopa je označena, fotograficky zadokumentována a následně zabalena do vhodného transportního obalu. Vytvoření zálohy a samotné zkoumání je následně realizováno na znaleckém pracovišti či v laboratoři znaleckého ústavu. Nejčastěji je tato metoda aplikována při zajišťování mobilní a komunikační techniky, jejíž zkoumání je z důvodu časové náročnosti vhodné provádět v laboratorních podmínkách a s dostatečným technologickým vybavením, případně při zajišťování takového druhu techniky, u kterého je zapotřebí provést komplexní zkoumání, a u kterého by bylo provedení zálohy či bitové kopie zatěžující z hlediska potřebného nestandardního technologického vybavení. [8]

Tento způsob zajištění stop je volen zejména v případech, kdy jsou zajišťovány:

- Mobilní telefony a jiná komunikační technika,
- Skimmovací zařízení u bankomatů,
- Odposlechová a špionážní technika,
- Plastové karty s magnetickým proužkem,
- Jednoúčelová a speciálně vyvinutá zařízení.

2.1.2 Zajištění stopy pomocí jednoúčelového technického zařízení

V této podkapitole bude rozebrán asi nejčastěji používaný způsob, pomocí kterého je možné pořídit bitové kopie zajištěných digitálních stop. Pod pojmem jednoúčelové technologické zařízení si lze představit přístroj, který byl speciálně vyvinut pouze pro pořizování bitových kopií ze stop, které jsou připojeny k jeho rozhraní. Toto zařízení bude v dalším textu blíže specifikováno. Další možností, jak lze chápat pojem jednoúčelového technologického zařízení je představa speciálně upraveného počítače, který je používán výhradně k těmto účelům. Často se jedná o desktop, který je osazen dostatečným počtem SATA kabelů pro připojení pevných disků (je vhodné, aby tento počítač obsahoval i starší typy konektorů, např. IDE). Takovýto technologický počítač by měl splňovat požadavky, které jsou kladeny na profesionální pracovní stanice. Použitým operačním systémem je v případě forenzního technologického počítače výhradně operační systém GNU/Linux (Fedora, Knoppix, Caine, Deft). Zde je potřeba podotknout, že není nutné používat pouze distribuce, které jsou speciálně určeny pro forenzní činnost. Využití operačního systému GNU/Linux má své hlavní opodstatnění ve spolehlivosti a bezkoliznosti systému, v možnosti rozsáhlé personalizace systému, a v neposlední řadě je použitím systému GNU/Linux zabezpečeno, že po připojení zkoumaného média k technologickému počítači nedojde k automatickému namountování tohoto média a k neautorizovanému zápisu systémových informací. Právě tato vlastnost je velice důležitá při práci s digitálními stopami – v okamžiku, kdy by po připojení k počítači došlo ze stany systému k zápisu jakýchkoliv systémových informací na disk (toto je vlastnost všech operačních systémů MS Windows), můžeme takto pozměněnou stopu považovat za znehodnocenou, jelikož došlo ke změně informací, které byly na předmětné stopě uloženy.

Pokud má výjezdová skupina k dispozici specializované zařízení pro vytváření bitových kopií (např. zařízení Tableau Forensic Duplicator), je použití tohoto přístroje a následné vytvoření bitové kopie libovolného harddisku, paměťové karty nebo USB paměti velice

snadné. Zařízení samotné je vybaveno vlastním operačním systémem a je zde zajištěna i ochrana proti zápisu. [5]

2.1.2.1 Použití zařízení k duplikaci disků:

- ze zájmového zařízení je vymontován pevný disk (případně je připraveno jiné médium, které je třeba zálohovat),
- jsou zjištěny základní parametry zkoumaného disku (velikost, výrobce, typové označení, výrobní a sériová čísla)
- z dostupného příslušenství je vybráno vhodné rozhraní, pomocí kterého bude zkoumaný disk připojen k zařízení. (nejčastěji je možno volit z redukcí: SATA, USB, IDE, SAS)
- k zařízení je připojen zkoumaný disk a disk technologický.
- Volbou v menu přístroje je nastavena konfigurace úkonů, které se budou provádět (wipe technologického disku, vytvoření bitové kopie, výpočet HASH)

Následně dojde k vytvoření bitové kopie zkoumaného média. Společně s bitovou kopií přístroj automaticky vytvoří i dokument, ve kterém jsou shrnuty veškeré informace o připojeném zkoumaném zařízení, postupu zálohování, a dále je připojena spočítaná HASH vytvořené zálohy. Po ukončení zálohování je možné zkoumané médium odpojit. Toto zařízení z mého pohledu velice usnadňuje samotnou práci na místě realizace. Hlavní výhodu spatřuji převážně v jednoduchosti ovládání a tzv. user friendly manipulaci, která je nepostradatelná zejména v okamžiku, kdy jsou úkony prováděny v prostředí s vysokou rušností či ve stresu, což může vést ke snadnému vzniku nežádoucích chyb.

Ne vždy musí ovšem výjezdová skupina zařízením typu Tableau Forensic Duplicator disponovat. V tomto případě je možno nahradit „duplikátor“ upraveným technologickým počítačem. Nejčastěji, jak bylo výše uvedeno, se pro toto zařízení hodí použít desktop s dostatečným počtem volných rozhraní pro připojení jednotlivých disků či ostatních médií, která chceme zálohovat. Toto zařízení by mělo disponovat také dostatečným výpočetním výkonem, aby bylo samotné zálohování co nejrychleji dokončeno. Takto upravený technologický počítač ve většině případů neobsahuje ani vlastní pevný disk. Při startu počítače je operační systém zaváděn často z připojené USB klíčenky, na které je nahrána tzv. „live“ distribuce některé z forenzních verzí systému GNU/Linux. Zde je důležité podotknout, že užití operačního systému GNU/Linux není podmínkou. Samozřejmě je možné na technologickém počítači provozovat i operační systém MS Windows či Mac OS

(pozn. Mac OS vychází ze systému GNU/Linux). V případě, že forenzní počítač používá pro svůj běh operačního systému MS Windows, je nezbytné, aby všechna zkoumaná zařízení byla k systému připojována s předřazeným blokátorem proti zápisu, jelikož OS Windows není na rozdíl od systému GNU/Linux defaultně nastaven do systému read-only, a mohlo by tak dojít k nežádoucímu zápisu na zkoumaný disk ze strany systému. Další podmínkou pro použití operačního systému MS Windows ve forenzní praxi je potřeba instalace specializovaného softwaru pro vytváření bitových kopií, jakým je např. software FTK Imager či EnCase.

2.1.2.2 Vytvoření bitové kopie pomocí technologického počítače se systémem GNU/Linux:

- ze zájmového zařízení je vymontován pevný disk (případně je připraveno jiné médium, které je třeba zálohovat),
- jsou zjištěny základní parametry zkoumaného disku (velikost, výrobce, typové označení, výrobní a sériová čísla),
- na základě zjištěných parametrů je vybrán vhodný technologický disk, na který bude provedeno zálohování,
- k vypnutému PC je připojen zkoumaný a technologický disk,
- technologické PC je zapnuto a dojde k zavedení operačního systému (volba linuxové distribuce, která bude pro zálohování použita, záleží pouze na našich preferencích a zkušenostech),
- po zavedení OS jsou provedeny kroky k vytvoření bitové kopie – přesný technologický postup viz kapiola 5.3.1.1,
- po ukončení zálohování je technologické PC vypnuto a zkoumané médium odpojeno.

2.1.3 Zajištění stopy pomocí zkoumaného zařízení

V praxi může nastat situace, kdy nebude možné použít pro vytvoření bitové kopie technologický počítač ani jiné jednoúčelové zařízení, či použití jmenovaných zařízení nebude doporučeno v zájmu zachování integrity stop. V takovém okamžiku je pořízení bitové kopie ralizováno na zajištěném, zájmovém, zařízení. Zejména se jedná o situace, kdy je v zájmovém zařízení nalezeno několik disků, které mohou být spojeny do tzv. RAID pole, a tudíž bychom se odpojením jednotlivých disků mohli dopustit jeho degradace. Další typickou situací, kdy je nutné použít pro vytvoření bitové kopie zajištěný systém, je případ,

kdy není možné provést demontáž počítače tak, aby mohl být vyjmut pevný disk. Často tato situace nastává u dnes moderních zařízení typu „netbook“ a „ultrabook“ či moderních pracovních stanic, tzv. „All in One“, kdy je celý hardware počítače umístěn za monitorem, který je s tělem počítače spojen nerozebiratelným, lepeným, spojem. Pro ilustraci lze jmenovat zařízení Apple iMac.

V okamžiku, kdy forenzní IT specialista na místě realizace dospěje k závěru, že pro pořízení bitové kopie je možno použít zajištěné, zájmové, zařízení, je technologický postup vytvoření bitové kopie prakticky identický s postupem, kdy je využíván jednoúčelový technologický počítač. Je třeba uvést, že v případě, kdy bude použit zajištěný počítač pro vytvoření zálohy jeho pevného disku, je důležité mít absolutní jistotu v tom, že po zapnutí počítače dojde k zavedení (nabootování) námi zvolené forenzní distribuce systému GNU/Linux. V opačném případě, tedy kdyby došlo k zavedení nainstalovaného operačního systému, došlo by tím i k nevratnému poškození systémových informací na disku počítače.

Pokud má forenzní IT specialista jistotu, že nedojde k nežádoucímu nabootování domovského operačního systému zajištěného počítače, je možno přistoupit ke vložení bootovacího média „live“ distribuce systému GNU/Linux a spustit počítač. Po úspěšném nabootování forenzního systému se k zajištěnému počítači připojí naformátovaný technologický disk a využitím výše uvedeného postupu je provedeno zálohování počítače a vytvoření bitové kopie. Technologický disk je k počítači připojen nejčastěji prostřednictvím USB - SATA redukce. Při použití tohoto druhu připojení je třeba počítat s delší dobou vytváření bitové kopie – ne z důvodu nízké výpočetní kapacity počítače, ale z důvodu přenosu dat pomocí USB rozhraní, jehož přenosová rychlost je oproti přímému napojení technologického disku na SATA sběrnici v případě použití forenzního počítače pomalejší.

2.1.4 Zajištění stopy ze spuštěného zkoumaného zařízení

Pořízení bitové kopie na spuštěném zařízení není, jak by se mohlo zdát, zdaleka neobvyklý úkon. Postupem času, a s čím dál více se rozšiřujícími možnostmi šifrování dat a využití nejrůznějších šifrovacích programů je tento druh činnosti na vzestupu. V případě, kdy je ověřeno, že na zájmovém počítači je aktivní některý ze šifrovacích nástrojů, je vždy výhodnější přistoupit k tomuto přístroji v okamžiku, kdy je zapnutý a tudíž je možno získat přístup k datům, která jsou nešifrovaná. U zapnutého počítače se nabízí data zálohovat pouhým vykopírováním na pevný disk, ale tento postup je z mého pohledu ne vždy dostačující. Vytvoření bitové kopie disku společně s pořízením otisku RAM paměti může

přinést pro další postup vyšetřování velmi cenné informace, které by pouhým vykopírováním souborů mohly zůstat skryty. Získání výpisu, neboli zálohy obsahu RAM paměti představuje pro další forenzní činnost získání cenného množství informací – v operační paměti se nacházejí informace o spuštěných procesech, obsahuje uživatelská data, ale také se zde nacházejí hesla a klíče v nešifrované podobě. Právě získání dekryptovacích klíčů je jedním z hlavních úkolů při pořizování otisku RAM paměti.

V otázce pořizování záloh bitových kopií na spuštěném systému však není možno opomenout i ostatní důvody, kdy by vypnutí systému nebylo žádoucí. Ve většině případů je přistupováno k vytvoření bitové kopie na zapnutém zařízení v případě potřeby vytěžení serverových úložišť. Zde je třeba podotknout, že zásah do spuštěného systému může provádět pouze osoba znalce či forenzního IT specialisty, která disponuje k tomuto úkonu potřebnými oprávněními.

2.2 Postupy zajišťování digitálních stop na místě činu

Tato podkapitola popisuje různé druhy digitálních stop, které se mohou na místě činu vyskytovat, a zároveň uvádí doporučené technologické postupy, které jsou využívány pro vytváření bitových kopií a záloh jednotlivých digitálních stop. Ne vždy však musí být digitální stopou konkrétní hardwarové zařízení – z toho důvodu jsou v rámci samostatné podkapitoly uvedeny varianty, kdy dochází k zajišťování zájmových dat.

2.2.1 Digitální stopy v podobě hardwarových zařízení

Stolní osobní počítače, pracovní stanice, notebooky či netbooky patří společně s přístroji mobilní a komunikační techniky k nejčastěji se nacházejícím zařízením na místě činu.

2.2.1.1 Stolní počítače, notebooky a servery

V rámci provádění úkonů trestního řízení jsou počítače zpravidla zajišťovány jako celek a poté následně odesílány ke znaleckému zkoumání. Periferní zařízení jako je klávesnice, myš, či monitor jsou ve většině případů ponechány majiteli – zajištění periferií je žádoucí pouze v případě, že se jedná o zařízení speciální, např. technologický počítač pro řízení výroby, apod. Na prvním místě, a v okamžik, kdy jsou zahájeny úkony trestního řízení, je zásadní, aby byla uživatelům zamezena jakékoliv další práce na počítači. Tímto opatřením jsme schopni minimalizovat možnost sabotáže, manipulace či mazání zájmových dat ze strany uživatele. Následně se provede zadokumentování místa nálezu počítače, včetně okolí. Je

doporučeno provést i dokumentaci periferií, zapojení kabeláže, atp. V případě, že je počítač spuštěn, je zásadní prohlédnout aplikace běžící na pozadí (šifrovací programy), zjistit, zda jsou na počítači namapována síťová úložiště a v neposlední řadě je doporučeno provést na místě zálohu RAM paměti. Pokud je provedena záloha RAM paměti a není na počítači spuštěno šifrování dat, je možné počítač vypnout. Proces samotného vypnutí počítače je ve většině literatury doporučen provést pouhým odpojením počítače od elektrické sítě, tzn. odpojit napájecí kabel ze zásuvky. V případě, že zajišťujeme počítač, který je ve vypnutém stavu, tak tento fotograficky zadokumentujeme, odpojíme od periferií a následně zajistíme pouze samotnou skříň počítače, ve které se nachází pevný disk. V žádném případě se vypnutý počítač nepokoušíme na místě zapnout a ověřit jeho funkčnost. V případě zajišťování notebooků či netbooků je nutné tyto zajistit i s napájecím adaptérem. V některých případech je možné zajistit ze zájmových počítačů pouze pevné disky, tento postup bychom však měli pečlivě zvážit zejména v okamžiku, kdy se v počítači nachází více pevných disků, které mohou být zapojeny v tzv. RAID poli, či mohou být disky šifrovány a toto šifrování je vázáno na hardware počítače, např. na jeho TPM čip. V takovém případě by bylo zajištění samotných disků prakticky bezcenné. U notebooků a netbooků je zajištění samotného pevného disku prakticky nedoporučováno.

Jedná-li se o zajišťování serverů, ve většině případů bereme v úvahu pouze zajišťování samotných dat, která jsou na místě realizace vykopírována na technologické disky a opatřena kontrolním součtem (MD5, SHA-1, apod.). V případě, že je nezbytné zajistit server jako celek, je aplikován stejný způsob zajištění, jako u běžného stolního počítače. Jedná-li se o externí pevné disky případně pevné disky, které jsou zasunuty v dokovací stanici, zajišťujeme je včetně jejich příslušenství (napájecí a datové kabely, či celá dokovací stanice). Zajištěné pevné disky je doporučeno vkládat do antistatických obalů a transportovat v obálkách, které ochrání obsah proti nárazu, na který jsou pevné disky náchylné a hrozilo by tak jejich poškození během přepravy. Není třeba zdůrazňovat, že všechny provedené kroky je třeba řádně protokolovat a do protokolu uvádět identifikační parametry zajištěných věcí, jako jsou typová označení, výrobní a sériová čísla, údaje o kapacitě, apod. [7]

2.2.1.2 Média pro uchování a přenos dat

Pod tuto skupinu zařízení můžeme zařadit veškerá optická média, jako jsou CD, DVD, BlueRay disky, ale také diskety, USB flash disky případně paměťové karty. Při provádění úkonů v rámci trestního řízení mohou být tato média nalézána v hojném počtu. Velmi

důležité je dbát na správnou identifikaci zejména USB flash disků. V současné době je na trhu nepřeberné množství zařízení, která svým provedením flash disk ani vzdáleně nepřipomínají, a mohou tak např. imitovat podobu hračky, přívěsku na klíče, či dokonce mohou vypadat jako šperk. Při zajišťování datových médií je doporučováno provést jejich roztřídění podle jednotlivých druhů, a místa, kde došlo k jejich nálezu. Následně se nalezená média očíslují, fotograficky zadokumentují a zabalí do obálek. Zároveň se provede zabezpečení obálek proti neoprávněné manipulaci. V případě USB flash disků je možné provést přímo na místě realizace jejich zálohování na vhodné technologické médium a zajistit tak pouze samotná zájmová data. Zálohování takového média je provedeno vytvořením jeho bitové kopie a spočítáním kontrolní sumy, aby byla zaručena integrita dat. Samozřejmostí je vedení pečlivé dokumentace a provedení záznamu do protokolu.

2.2.1.3 Mobilní a komunikační technika

Mobilní a komunikační technika dnes patří mezi jedny z nejčastěji zajišťovaných zařízení. V ideálním případě je doporučeno se samotným přístrojem zajistit i napájecí adaptér s kabelem a od dotčené osoby získat přístupová hesla. Zde, pokud nám dotčená osoba dobrovolně sdělí PIN kód ke svému mobilnímu telefonu, či tabletu platí, že toto přístupové heslo musí být vyzkoušeno, a po jeho ověření zaprotokolováno.

Postup zajištění mobilního telefonu či tabletu je téměř analogický jako u zajišťování ostatní techniky. V zásadě rozlišujeme pouze mezi tím, zda přicházíme k zapnutému nebo vypnutému přístroji. V případě prvním, kdy je přístroj zapnutý, aktivujeme v prvním kroku tzv. režim „letadlo“, který je pro dnešní smartphony zcela běžný. Aktivací tohoto režimu docílíme odpojení přístroje nejen od mobilní sítě, ale i od Wi-Fi. V tuto chvíli máme jistotu, že zajištěný přístroj nemůže být vzdáleně ovládán a nemůže tak například dojít k úmyslnému smazání jeho obsahu za pomoci vzdálené správy. Dále je zapotřebí se ujistit, že jsme deaktivovali veškeré bezpečnostní a přístupové prvky a v případě, že telefon vypneme, nebude při jeho opětovném zapnutí požadován kód PIN. V ojedinělých případech je nezbytné, aby byl telefon po celou dobu zkoumání zapnutý. V takovýchto případech přístroj zajistíme i s napájecím kabelem, který vyvedeme ven z bezpečnostního obalu. Zde je zapotřebí zdůraznit, že mobilní telefony, tablety a obdobné přístroje ukládáme vždy do bezpečnostních obalů, které jsou vyrobeny z neprůhledného materiálu. Tímto zabráníme neoprávněné manipulaci s přístrojem. V okamžiku, kdy se rozhodneme telefon či jiný

přístroj transportovat ve vypnutém stavu, je doporučeno po vypnutí přístroje vyjmout baterii a SIM kartu. [4]

2.2.1.4 Síťové prvky

Aktivní síťové prvky, jako jsou routery, access pointy či firewally jsou zajišťovány téměř ojediněle. V případě, že je však nezbytné tato zařízení zajistit, je na prvním místě rozhodnutí, zda zajistit zařízení jako celek, či přistoupit pouze k vykopírování provozních dat. Jednou z otázek, kterou si je při tomto rozhodování vhodné položit je, zda u daného zařízení nedojde po jeho vypnutí k nevratné ztrátě obsahu jeho paměti. Vzhledem k tomu, že většina aktivních síťových prvků nabízí možnost administrace pomocí síťového připojení, jeví se jako vhodnější varianta provést zálohu těchto zařízení na místě. V tomto případě bude ovšem nezbytná spolupráce administrátora sítě, který je důkladně obeznámen s její topologií, a pomůže nám získat přístupy do zájmových zařízení. Celý postup je vhodné dokumentovat minimálně pomocí fotografií. Samotný obsah paměti zařízení můžeme poté zajistit několika způsoby. Jako nejjednodušší se jeví fotografické zadokumentování současného stavu nastavení, případně pořízení snímků obrazovky, na kterých bude zachyceno aktuální nastavení, příp. další provozní informace, logy, atp. Jako další varianta se nabízí pořízení bitové kopie paměti, pokud to dané zařízení umožňuje. Všechna zajištěná data je nutné opatřit kontrolním součtem pro následnou verifikaci a tato data nepřepisovatelně uložit na technologické médium. O celém postupu je opět zpracován záznam do protokolu.

2.2.1.5 Ostatní elektronika

Pod pojem ostatní elektronika můžeme zahrnout ta zařízení, která nejsou tak často předmětem zájmu vyšetřovatelů, ale která mohou v některých případech obsahovat potřebné digitální důkazní materiály. Z těch nejčastěji používaných to mohou být např. digitální fotoaparáty, elektrické psací stroje, tiskárny a skenery, videorekordéry, atp. Před zajištěním těchto zařízení je nutné se zabývat otázkou, zda je z těchto zařízení vůbec reálné nějaké důkazní materiály získat a také, zda při zajišťování těchto zařízení nedojde k poškození nebo ztrátě zájmového záznamu. V případě, že se takovéto zařízení zajišťuje, je doporučeno společně s daným přístrojem zajistit i napájecí kabeláž s adaptérem, propojovací kabely a další součásti nezbytné k provozu.

Postup zajištění těchto zařízení je prakticky identický jako u výše uvedených. O všech provedených krocích vedeme video či fotografickou dokumentaci, zajištěné stopy balíme do bezpečnostních obalů a zapisujeme do protokolu. [7]

2.2.2 Digitální stopy v podobě zájmových dat

Zajištění samotného obsahu, čili dat, je další z variant zajištění digitálních stop. K tomuto kroku je v současné době přistupováno zvláště v případech, kdy jsou zájmová data získávána ze serverů. Velmi často se totiž stává, že jsou data uložena na vzdáleném serveru, který se nachází mimo hranice objektu, ve kterém jsou prováděny úkony v rámci trestního řízení. Může však také nastat situace, že na daný server má zřízen přístup více subjektů, v takovém případě je zcela nemožné server zajistit in natura, jelikož by mohlo dojít k poškození třetích osob, které s danou trestní věcí nemusí mít nic společného. Poslední, velmi často se vyskytující variantou je situace, kdy na jednom fyzickém serveru běží několik serveru virtuálních. I v tomto případě je výhodnější zajistit na místě pouze zájmová data. Zajišťování dat, a zásah do živého systému je oprávněna provádět pouze osoba znalce, či osoba, které k tomuto kriminalisticko-technickému úkonu byla řádně proškolena. V dalším textu jsou uvedeny příklady nejčastěji zajišťovaných dat:

2.2.2.1 E-mailové zprávy a elektronická komunikace

E-mailové zprávy a ostatní elektronickou komunikaci zajišťujeme zásadně v digitální podobě. Pouze s takto zajištěnou zprávou může znalec dále pracovat – kromě samotného obsahu je pro odborné zkoumání více důležité to, co běžný uživatel nevidí, tedy záhlaví a zápatí zprávy, které s sebou nese informace technického charakteru. Zprávy a elektronickou komunikaci je možno zajistit jak v rámci domovní prohlídky u osoby podezřelé, tak například je možné zprávy zajišťovat u osoby oznamovatele či poškozeného. V tomto případě je celý proces realizován za souhlasu poškozeného, a děje se tak v případech, kdy je podezření na spáchání trestného činu na internetu, jako např. podvodu, rozesílání výhružných e-mailů, phishingu, stalkingu, apod. [12]

Postup zajišťování e-mailových zpráv je možno shrnout v několika bodech:

- Zprávy jsou zajišťovány přímo přes webové rozhraní nebo e-mailového klienta z účtu pachatele či poškozeného,
- Zprávy jsou zajišťovány ve formátech: .pst, .ost, .eml, .msg, případně pokud to není technicky možné, tak zprávy zajišťujeme vždy se záhlavím,

- Zprávy zajišťujeme výhradně v elektronické podobě,
- Zajištěná data jsou vždy verifikována pomocí kontrolního součtu, nejčastěji volíme MD5, SHA-1 nebo SHA-2,
- Zajištěná data jsou uložena na nepřepisovatelné technologické médium,
- Zajišťovat lze pouze originál zprávy, tedy ne tu zprávu, která byla přeposlána. U přeposílané zprávy dojde ke ztrátě technických dat v záhlaví.

V záhlaví e-mailové zprávy nalézáme informace o samotném putování zprávy. Tedy, kterým e-mailovým serverem byla zpráva odeslána, v kolik hodin byla odeslána, přes které další servery procházela, ale také komu dalšímu byla zpráva určena a z jakého poštovního klienta odeslána. Nejcennější informací je však samotná IP adresa, ze které byl e-mail odeslán. Podle IP adresy je možno určit konkrétní počítač, ze kterého byla zpráva odeslána. [3]

2.2.2.2 Webové stránky a webové servery

Webové stránky patří mezi nejčastěji zajišťovaná data v rámci provádění úkonů trestního řízení. V zásadě jsou data z webu zajišťována v rámci volně přístupných zdrojů na Internetu, nebo mohou být zajišťována z Intranetových stránek různých společností. To, zda se jedná o data z veřejného Internetu, či soukromého intranetu může indikovat na množství a rozsah zajištěných dat, který dělíme na:

- Jednotlivé webové stránky – diskuse na sociálních sítích, profil na Facebooku, apod.,
- Stránky jsou zajištěny z celého obsahu konkrétní domény – stránky oranizace, e-shop, apod.,
- Kompletní zajištění dat webového serveru, včetně zdrojových kódů, grafiky, apod.

Zajišťování tohoto druhu stop má také svůj technologický postup, kterým je třeba se řídit.
Postup zajištění webových stránek:

- Zájmová stránka je načtena do prohlížeče,
- Stránka je zadokumentována (fotograficky nebo pomocí snímku obrazovky),
- Webová stránka je zálohována přímo z webového prohlížeče, případně se pro její uložení použije některý z volně dostupných nástrojů, jakým je např. Website Copier,
- Pro veškerá vykopírovaná data je vypočtena suma kontrolního součtu HASH – nejčastěji jsou použity algoritmy MD5, SHA-1 nebo SHA-2,
- Veškerá vykopírovaná data jsou uložena na nepřepisovatelné médium společně s kontrolními součty, které byly k vykopírovaným datům pořízeny,

- Postup je zapsán do protokolu, ve kterém je specifikováno, jaké úkony byly provedeny, je zde uvedena základní charakteristika dat, která byla zajištěna a zároveň jsou v protokolu uvedeny i vypočtené kontrolní součty pro zpětnou verifikaci.

Postup zajištění obsahu domény:

- Pomocí webového prohlížeče je načtena zájmová doména,
- Použitím specializovaného softwaru dojde k postupnému uložení obsahu celé domény (v nastavení softwaru lze konfigurovat, jaký rozsah má být zajištěn),
- Zajištěná data jsou verifikována pomocí otisku kontrolního součtu HASH,
- Data jsou vykopírována na nepřepisovatelné médium společně s vypočtenou kontrolní sumou,
- Postup je zapsán do protokolu, ve kterém je specifikováno, jaké úkony byly provedeny, je zde uvedena základní charakteristika dat, která byla zajištěna a zároveň jsou v protokolu uvedeny i vypočtené kontrolní součty pro zpětnou verifikaci.

Variantou nejnáročnější nejen na čas, ale i na objem dat je zajišťování obsahu webového serveru. Takovéto zajišťování dat bývá nejčastěji iniciováno na základě probíhajících úkonů v rámci trestního řízení. Zpravidla jsou takovéto servery provozovány v komerčních společnostech zabývajících se webhostingem. Poskytovatelé hostingu také nejsou ve většině případů v trestní věci nijak interesováni, což ujednodušuje celý proces dobrovolného vydání dat. [3]

V případě, že jsou zajišťována data z webového serveru, je doporučeno, dodržovat níže uvedený postup:

- Zjistit typ a verzi používaného web serveru a platformu, na které je server spuštěn,
- Zjistit, jakou strukturu mají uložená data,
- Získat a zaprotokolovat přihlašovací údaje a přístupová hesla (administrátosrská),
- Za použití vhodného nástroje, jakým je např. FTK Imager, provést zálohování všech zájmových dat na technologický disk,
- Na technologický disk provést zálohu provozních logů,
- Zajištěná data opatřit kontrolními součty HASH pro jejich verifikaci,
- Technologický disk řádně označit, v průběhu provádět fotodokumentaci,
- Zpracovat protokol a uvést do protokolu základní informace o charakteru zajištěných dat včetně kontrolních součtů HASH.

2.2.2.3 Databázové servery

Problematika zajišťování databázových serverů je v rámci zajišťování digitálních stop velmi úzce specializovanou činností, u které se v žádném případě neobejdeme bez zkušeného specialisty, který je s problematikou databází dobře seznámen. Ve většině případů bude také nezbytné, aby byl při procesu zajišťování přítomen administrátor, případně správce databázového serveru. V okamžiku, kdy je nezbytné zajistit data z databázového serveru, je výhodnější provést jeho zálohu, a tedy data vykopírovat pomocí vhodného nástroje na technologický disk. V takovémto případě je vhodné použít např. softwarový nástroj FTK Imager, který provede zálohu celého serveru, případně jeho vybrané části a výstup uloží do forenzního formátu .E01, což je velice výhodné pro další práci s daty, zejména, jsou-li načtena do některého z forenzních programů, jako je EnCase, X-Way či BlackLight. V krjních případech může dojít i k zajištění celého databázového serveru – k tomuto je většinou přistoupeno v okamžiku, kdy majitel serveru, jeho administrátor případně správce odmítají spolupracovat a věc vydat dobrovolně, nebo když se vyskytnou technické potíže a není zaručeno, že by data ze serveru byla zajištěna korektně a bez chyb. Databáze ovšem nemusí být vždy umístěny na serveru, některé typy databází mohou být spuštěny i na lokálních počítačích. Typickým příkladem lokální databáze mohou být Microsoft Access. Na samotných serverech se poté velmi často setkáváme s databázemi Microsoft SQL či s produktem společnosti Oracle MySQL. Je také nutno podotknout, že v případě, kdy chceme zajišťovat data z jakéhokoliv databázového serveru, měli bychom znát jeho lokalizaci v rámci topologie sítě. Server jako takový totiž vůbec nemusí být umístěn v daném objektu, ale může se nacházet i stovky kilometrů daleko. [3]

Zajišťování dat ze serverů je ve většině případů prováděno z počítače správce sítě či administrátora systému přes speciální rozhraní. V případě, že je zajišťována lokální databáze, která se nalézá na disku konkrétního počítače, je postup zajištění velice snadný. Lokální databáze musí být fyzicky identifikována na konkrétním počítači v síti. Poté je připraven technologický disk, který se následně připojí k počítači. Následně se provede vykopírování veškerých dat z předmětné databáze na připravený technologický disk, a ze zajištěných dat jsou spočítány kontrolní sumy neboli HASH souborů. Technologický disk je třeba řádně označit a zaprotokolovat celý postup včetně uvedení kontrolních sum do protokolu. [4]

V případě, kdy jsou zajišťovány celé databáze umístěné na databázovém serveru, je možno postupovat následovně:

- Zjistit typ a verzi používaného databázového serveru včetně platformy, na které je server spuštěn,
- Zajistit přihlašovací údaje a administrátorská přihlašovací hesla,
- Zjistit, jak a v jaké formě jsou data uložena a jak jsou strukturována,
- Přes administrační rozhraní provést přihlášení k databázovému serveru (pozn. k tomuto a k následujícím krokům je doporučeno přizvat i administrátora nebo správce serveru, který je ochoten spolupracovat a má povědomí o struktuře dat a administraci samotného serveru,
- Provést, přes administrační rozhraní, vytvoření úplné zálohy zájmové databáze. Případně použít některý z forenzních nástrojů, které tuto funkci obsahují a vytvořit kompletní tzv. „dump“ databáze. Zásadní v tomto kroku je zajistit opravdu všechna data a součásti, které se k dané databázi vztahují.
- Výsledná záloha musí být opatřena vypočteným kontrolním součtem pro následnou verifikaci dat.
- Veškeré kroky je vhodné fotograficky dokumentovat,
- Data jsou uložena na technologický disk, případně na jiné vhodné médium a dále jsou opatřena otiskem HASH,
- Médium, na kterém jsou data uložena, je označeno a zaprotokolováno. Stejně tak jsou do protokolu uvedeny hodnoty kontrolního součtu HASH a identifikační údaje o technologickém disku.

Speciálním případem, kdy je zajišťována konkrétní databáze z databázového serveru může být například zajištění účetních dat. Ve většině případů jsou účetní data elektronicky zálohována i za několik let zpětně, a proto se jedná o databáze velmi rozsáhlé, které navíc „běží“ na specializované platformě speciálních účetních programů. V okamžiku, kdy je nutné zajistit data z účetního serveru, je nanejvýš vhodné, abychom vyselektovali pouze data, která se vztahují k zájmovému období, tedy data z určitých let. Selekci konkrétních zájmových dat může na místě, kde probíhají úkony trestního řízení provést vyšetřovatel, popřípadě ve složitějších případech je možno přibrat znalce z oboru účetnictví, který bude s případem seznámen, a navrhne, která data jsou k danému případu relevantní.

Při zajišťování účetních dat se můžeme setkat s několika scénáři, podle kterých zvolíme, jak budeme postupovat. V první fázi je důležité zjistit, v jakém účetním programu jsou data archivována. V případě, že se jedná o volně dostupný, nebo komerčně nabízený program, je možné vykopírovat pouze zájmová data. V případě druhém, kdy je účetnictví vedeno ve speciálně vyvinutém programu, který byl vytvořen např. dotčenou osobou, je nutné zajistit celou databázi, což může v extrémním případě znamenat i zajištění několika TB dat.

Postup zajištění dat je možno shrnout do několika bodů:

- Zjistit, jaký účetní software je používán, tzn. výrobce, verze, technické parametry a požadavky,
- Získat přihlašovací údaje a administrátorská přihlašovací hesla,
- Na technologický disk vykopírovat veškeré adresáře vztahující se k danému účetnímu programu,
- Provést přihlášení do systému a za spolupráce uživatele vytvořit plnou zálohu zájmových dat, včetně záloh,
- Ze všech vykopírovaných dat zajistit kontrolní sumy MD5, SHA-1 nebo SHA-2,
- Veškerá data uložit na nepřepisovatelné médium, nebo jiné technologické médium včetně kontrolních součtů,
- Vše řádně zaprotokolovat a fotograficky zadokumentovat.

2.3 Taktika zajišťování digitálních stop na místě činu

V případě ohledání materiálního místa činu platí pravidlo, které hovoří o tom, že při samotném zajišťování výpočetní a komunikační techniky, či ostatních digitálních stop se nelze soustředit pouze na tyto stopy, ale je zapotřebí věnovat pozornost i jejich nejbližšímu okolí. V extrémních případech může být tato pozornost věnována např. i odpadkovému koši umístěnému pod stolem. Před samotným započetím domovní prohlídky či prohlídky jiných prostor je více než doporučeno předem specifikovat, jaké digitální stopy jsou pro vyšetřování zájmové a na kterých místech by se mohly nalézat. Pokud bude prohlídka probíhat např. v kanceláři podezřelého či pachatele, primární zájem bude směřovat na pracovní stůl a samozřejmě na bezprostřední okolí pracovního stolu, kde bude koncentrace digitálních stop největší. Prohlídka tohoto prostoru by však neměla strhnout veškerou pozornost, jelikož důkazní materiál, v podobě digitálních stop, se může nacházet i na ostatních místech kanceláře. Kromě zkoumání samotného počítače na pracovním stole by tak měla být

prozkoumána nejen periferní zařízení, která jsou k němu připojena, ale také vytištěné dokumenty v tiskárně, poznámky na pracovním stole a na nástěnce, či otevřené a rozpracované dokumenty v počítači. Právě zde se mohou mnohdy nacházet důležité informace, které se k vyšetřovanému případu mohou vztahovat. [1]

V některých případech je z taktického hlediska nezbytné, aby byl zájmový počítač zapnutý. Jedná se zejména o situace, kdy osoba pachatele či podezřelého aktivně využívá některý ze šifrovacích nástrojů, jako je např. komerčně dostupný TrueCrypt či BitLocker. Ve druhém případě, kdy je nezbytné z taktických důvodů přistupovat k zapnutému „živému" systému, je potřeba přístupu k datům, která mohou být uložena na vzdáleném serveru či na některém z cloudových úložišť. Z tohoto důvodu je třeba věnovat pozornost nejen spuštěným procesům, které běží na pozadí systému, ale měli bychom se věnovat také připojeným síťovým prvkům, kterými mohou být např. NAS servery, a v neposlední řadě bychom neměli opomenout přítomnost Wi-Fi sítí. V případě přítomnosti Wi-Fi sítě, a jsou-li k ní zařízení připojena, je vhodné, pokud to situace umožňuje, veškerou výpočetní a komunikační techniku od této sítě odpojit, aby se zamezilo vzdálenému přístupu k zájmové technice. U mobilních a komunikačních zařízení je doporučeno je převést do tzv. režimu „letadlo", kdy dojde k odpojení ode všech datových sítí a služeb, aby bylo zamezeno vzdálenému smazání dat z těchto zařízení.

Samozřejmostí by před zahájením jakýchkoliv úkonů mělo být i posouzení bezpečnostního rizika, které může v průběhu činnosti hrozit. Zde by mělo být myšleno nejen na zabezpečení místa, kde je úkon prováděn, ale hlavně na bezpečnost samotných účastníků.

V průběhu zajišťování digitálního důkazního materiálu a stop je důležité postupovat velmi systematicky a koordinovaně, aby bylo zamezeno zničení digitálních stop, ať úmyslného ze strany pachatele či nedbalostního ze strany policejního orgánu. V tomto případě může sehrát svou roli i tzv. moment překvapení. Jeho využitím můžeme nad pachatelem získat významnou taktickou výhodu. Nejen, že minimalizujeme možnost úmyslného zničení zájmových dat a důkazů, ale také můžeme v rámci neodkladnosti a neopakovatelnosti úkonu bezprostředně přistoupit k „živému" systému tak, jak jej využívá pachatel, a tím pádem se lze domnívat, že v daném okamžiku budou na zájmovém zařízení spuštěny všechny služby a připojena všechna síťová zařízení. V případě, že budeme přistupovat k „živému" systému, je nezbytné poukázat na skutečnost, že k provádění jakýchkoli kriminalisticko-technických úkonů jsou oprávněni pouze kriminalističtí či civilní znalci, popř. proškolení policisté, kteří

mají oprávnění k zajišťování výpočetní techniky, pořizování bitových kopií a k provádění dalších nezbytných kriminalisticko-technických úkonů. [9]

Při provádění úkonů dle trestního řádu je nezbytné pro potřeby forenzní analýzy zjistit následující informace:

- počet počítačů a jejich typové označení,
- používané operační systémy,
- zapojení počítačů do sítě LAN a informace o topologii této sítě,
- typ a množství používaných záznamových médií,
- zjištění vzdálených úložišť a užívaných cloudových služeb,
- zjištění specializovaného SW vybavení počítačů.

V dnešní době je v celku běžné, že velké firmy využívají pro správu své IT infrastruktury smluvní společnosti či externí zaměstnance a zároveň využívají velmi moderní a vyspělé technologie. V takovýchto případech je při zajišťování digitálních stop prakticky nezbytná spolupráce s počítačovými experty dodavatelské společnosti. Při této součinnosti je následně prováděno veškeré zajišťování digitálních stop za dohledu kriminalistického IT specialisty či kriminalistického znalce.

Z taktického hlediska je v rámci přípravy před samotným zahájením zajišťování digitálních stop doporučeno provést následující:

- Na základě získaných informací o případu vyvodit, jaké digitální stopy se budou pravděpodobně zajišťovat a jakým způsobem.
- Získat informace o druhu informačních a komunikačních zařízení, která se na místě realizace mohou či budou vyskytovat. Zde se jedná o množství a rozmístění techniky, přítomnosti serverů, odhadu objemu zajišťovaných dat, a samozřejmě o užívání specializovaného SW nebo HW vybavení. V rámci tohoto kroku můžeme získat představu o počítačové gramotnosti a odbornosti pachatele, personálu, o používaných bezpečnostních opatřeních či nasazení kryptografických metod.
- Zhodnotit včasnost prováděného úkonu. Čím dříve jsou úkony prováděny, tím lépe vzhledem k možné ztrátě digitálních stop např. smazáním a následným přepsáním.
- Připravit dostatečné technické vybavení – zde se jedná především o dostatečnou kapacitu pevných, technologických disků, na které budou data nahrána, ale také příprava technologických počítačů a výjezdového vybavení.

- V případě použití zcela nové, nebo specifické technologie, zajistit přítomnost specialisty na tuto problematiku na místě realizace. Přítomnost odborníka je nezbytná pro konzultaci optimálního postupu zajištění dat tak, aby se eliminovalo jejich poškození či ztráta.
- Zhodnotit, zda provedení nezbytných úkonů nebude mít neblahý dopad na činnost dalších firem a organizací a procesem zajištění digitálních stop tak nedojde k zásahu do práv třetích osob.

Do procesu přípravy před zajišťováním digitálních stop je možno zahrnou i provádění operativní činnost, na jejímž základě je možné získat přístupová hesla k počítačovým systémům, získat informace o použitém šifrování souborů či zjistit další důležité skutečnosti, které mohou být pro naši činnost rozhodné. Pokud je to možné, za velmi přínosné lze považovat získání informací od správců sítě či administrátorů systému, kteří nám mohou poskytnout své znalosti o používaných informačních a databázových systémech nebo přístupových heslech. Obecně lze říci, že jakékoliv, předem získané informace, následně usnadní provádění všech úkonů souvisejících se zajišťováním digitálních stop.

2.4 Dokumentace a balení zajištěných stop

V rámci provádění úkonů ve smyslu zákona č. 141/1961 Sb., o trestním řízení soudním je v dikci tohoto zákona orgánům činným v trestním řízení uloženo, aby byl celý postup prováděných úkonů, včetně zajišťování digitální techniky a stop, řádně dokumentován.

Druhy dokumentace při zajišťování stop:

- písemně protokolem dle zvláštního právního předpisu,
- fotografickou dokumentací,
- videodokumentací, která je doplněna o slovní popis policisty,
- topografickou dokumentací (plánkem, náčrtkem)

2.4.1 Požadavky na dokumentaci digitálních stop

Veškeré objekty, které jsou v rámci prováděných úkonů zajišťovány, a které by mohly obsahovat digitální stopy, je nutné do příslušného protokolu podrobně popsat tak, aby byly jednoznačně rozpoznatelné a nemohlo dojít k jejich záměně. K tomuto účelu je každý zajišťovaný objekt důkladně popsán do protokolu, a obsahuje-li na sobě např. uvedené výrobní číslo, i toto je do protokolu zaznamenáno. V zásadě se dá hovořit o tom, že do

protokolu uvádíme údaje, které objekt identifikují tzv. druhově, což jsou údaje o výrobci, modelu, tvaru, barvě, způsobu použití, atd. Dále také uvádíme údaje, které mohou vést k tzv. individuální identifikaci. Za tímto účelem vyhledáváme markanty, které jsou pro daný objekt jedinečné, jako jsou např. sériová čísla, výrobní a identifikační čísla, ale také vrypy, škrábance a další speciální označení. Společně se slovním popisem daného objektu je pořízena i jeho fotodokumentace a objekt je zapsán do protokolu, kde je mu přiřazeno číslo stopy, které koresponduje s číslem, které je uvedeno vedle objektu na fotografii. [5]

Protokoly upotřebitelné v rámci provádění úkonů trestního řízení.:

- protokol o ohledání místa činu, dle § 113 trestního řádu,
- protokol o provedení domovní prohlídky, dle § 82 trestního řádu,
- protokol o provedení prohlídky jiných prostor a pozemků, dle § 82 trestního řádu,
- protokol o odnětí věci, dle § 79 trestního řádu,
- protokol o vydání věci, dle § 78 trestního řádu. [2]

V okamžiku, kdy jsou zahájeny úkony v rámci trestního řízení, je nanejvýš vhodné, aby před samotnou prohlídkou zájmových prostor došlo k fotografickému zadokumentování současného stavu. To znamená, že každé místo, které bude prohlíženo, je nejprve zodokumentováno tak, jak bylo nalezeno.

Dokumentace samotná hraje svou nezastupitelnou roli v rámci dokladování legálnosti celého postupu a nezpochybnitelně zachycuje reálnou situaci na místě, kde jsou prováděny úkony v rámci trestního řízení.

Jak již bylo výše uvedeno, před samotným započetím zajišťování jakékoliv výpočetní techniky, datových nosičů, nebo jiných elektronických součástek je nezbytná jejich fotografická dokumentace. Jedná-li se např. o techniku, která je nalezena na pracovním stole, je vhodné pořídit přehledovou a polodetailní fotografii daného pracovního stolu a na něm uložené techniky, včetně rozmístění jednotlivých přístrojů. Dále, nachází-li se na pracovním stole počítač, tiskárna, NAS server, nebo jiné zařízení, které je připojeno k rozvodné a datové síti, provede se i dokumentace kabeláže, která je k těmto zařízením vedena.

V okamžiku, kdy jsou jednotlivá zařízení zajišťována, je jim přiděleno konkrétní a jedinečné číslo stopy, které je k zařízení přiloženo při fotografování a s tímto číslem je zařízení uvedeno do protokolu jako stopa. Dále je do protokolu zaznamenáno označení výrobce,

model, výrobní a sériové číslo daného zařízení tak, aby toto zařízení bylo kdykoliv jasně identifikovatelné.

V případě, kdy se na místě činu nacházejí elektronické zařízení, která jsou spuštěná, je možné provést fotografickou dokumentaci obsahu, který je na ploše či displeji zařízení. [6]

2.4.2 Požadavky na ukládání digitálních stop

Neméně důležité, v porovnání se samotnou dokumentací stop a průběhu činnosti na místě činu, je i samotné balení zajištěných digitálních stop, které má svá přísná pravidla. V okamžiku, kdy je zajišťován objekt, který má charakter elektronického zařízení, nebo paměťového média, na kterém jsou uložena zájmová data, je třeba takovýto objekt dostatečně zabezpečit proti neoprávněné manipulaci. Veškerá digitální data jsou v tomto ohledu velmi křehké zboží, a proto je nezbytně nutné při jejich zajišťování důrazně dbát na to, abychom se vyvarovali jakýchkoliv procesních chyb, které by mohly zvrátit směr vyšetřování a zhatit tak i několik let usilovné práce. V praxi jsou proto veškeré digitální stopy baleny a ukládány do speciálně určených obalů, které jsou schopny zabezpečit stopy proti poškození – mechanickému nebo fyzikálnímu. Některé obaly, používané např. pro mobilní techniku, mohou fungovat i jako Faradayova klec, aby byla přenášená technika chráněna před neautorizovaným přístupem pomocí bezdrátové sítě. [5]

2.4.3 Prostředky určené pro ukládání zajištěných stop

- číslované obaly s bezpečnostní pečetí ORGATECH,
- plastové pytle opatřené bezpečnostní plombou,
- papírové pytle různých velikostí,
- lepenkové krabice,
- původní obaly od zajišťované techniky.

V případě, že jsou zajištěné stopy ukládány do k tomuto účelu speciálně navržených obalů, je součástí tohoto obalu i mechanismus, pomocí kterého je možno jasně identifikovat, že mohlo dojít k neautorizovanému přístupu k zajištěné stopě. Pokud jsou stopy ukládány do běžných papírových pytlů, lepenkových krabic či původních originálních obalů, je pro zabezpečení stopy důležité, aby byl tento transportní obal dodatečně zabezpečen lepicí páskou v místech, kde jsou spoje materiálu, a také v místech, která by bylo možno bez jejich zjevného porušení otevřít a následně zavřít. Takovéto opatření je doplněno o razítko policejního orgánu, který zajištění stopy provedl – toto razítko je otisknuto na několika

místech, vždy na přechodu mezi materiálem obalu a lepenky a dále je stejným způsobem připojen i podpis osoby, která zajištění provedla, dále podpis dotčené osoby a nakonec podpis nezúčastněné osoby. Celý způsob, kterým je obal zabezpečen, je nutno uvést do protokolu a následně fotograficky zadokumentovat.

Samotné obaly je následně nutno označit tak, aby byla na první pohled možná identifikace obalu (z důvodu záměny) a také, aby bylo zřejmé, ke které trestní věci se dané stopy vztahují, K tomuto účelu se na obaly uvádí zejména údaje o čísle jednacím, dále je přiložen popis uloženého objektu, místo kde byl zajištěn, číslo stopy o kterou se jedná apod. Tyto údaje se uvádí nesmazatelným popisovačem přímo na bezpečnostní obal, případně je možno použít předtištěné samolepící štítky.

Nezastupitelnou úlohou bezpečnostního obalu není pouze ochrana vloženého objektu před neoprávněnou manipulací. Bezpečnostní obal plní také funkci protektivní, aby nedošlo k poškození zabalené stopy. V případě balení magnetických médií je vhodné, aby byly použity obaly chránící před účinky elektromagnetického pole, nebo v případě, kdy jsou balena optická média, je nezbytné tato balit do obalů, které jsou neprůhledné tak, aby byly minimalizovány účinky UV záření. Jako poslední je možno uvést specifikum balení mobilní a komunikační techniky, která se v ojedinělých případech může zajišťovat a následně transportovat v zapnutém stavu. Z tohoto důvodu je nezbytně nutné, aby se veškerá tato technika balila do neprůhledných obalů a to z důvodu zabránění čtení informací z displeje telefonu. Velmi problematická se poté jeví myšlenka, že by ze zapečetěného obalu měl vést napájecí konektor s adaptérem. Tato varianta je možná pouze v případě, že samotný adaptér a napájecí kabel jsou pevně spojeny v jeden celek. V případě, který je v dnešní době velmi častý, kdy napájecí adaptér je od samotného kabelu oddělitelný, a tyto dvě součásti jsou mezi sebou spojeny pomocí rozhraní USB, je tato myšlenka balení nereálná, a to právě z důvodu velmi snadného přístupu k datům, která jsou v telefonu uložena, bez toho aniž by bylo třeba porušit bezpečnostní obal. V takovéto situaci se nabízí dvě varianty. Prvním možným řešením je použít pro napájení neoriginální technologickou kabeláž, kde bude adaptér a samotný napájecí kabel pevně spojen v jeden celek a může tak být konec s adaptérem volně vytažen z bezpečnostního obalu. Druhou variantou, kterou je možno v takové situaci aplikovat by poté bylo připojení telefonu na powerbanku s dostatečnou kapacitou, a telefon tak společně s externí baterií transportovat v zapečetěném obalu bez nutnosti vývodu kabeláže.

Problematika zajišťování, balení a ukládání stop má také svůj význam v okamžiku, kdy je nutno zajistit objekt, který je složen z několika technologicky oddělitelných částí. V takovém případě by bylo velmi složité každou část popisovat zvlášť, a proto je objekt (např. stolní počítač) vždy zajišťován jako jeden nedělitelný celek. Toto opatření vychází také z toho důvodu, aby bylo předejito problémům, které by mohly nastat při vracení techniky zpět majiteli. Právě z tohoto důvodu je technika jako celek zajišťována a také je jako celek vracena. [4]

II. PRAKTICKÁ ČÁST

3 RIZIKA PRÁCE S DIGITÁLNÍMI STOPAMI

Kapitola je věnována zmapování procesu práce s digitálními stopami a snaží se zmapovat možnosti vzniku chyby při vytváření záloh zajištěných stop vlivem nedodržení doporučených technologických postupů. Tato kapitola si klade za cíl identifikovat možná rizika a ohrožení, která v průběhu práce s digitální stopou mohou nastat. Ke každému identifikovanému riziku či ohrožení je dále navrhnuto protiopatření na zmírnění či eliminaci možných následků. V ideálním případě by mělo dodržení navrhovaného protiopatření vést ke stavu, kdy budou veškerá rizika potlačena na minimum, a nebude tak hrozit znehodnocení stopy vlivem nesprávné manipulace či technologického pochybení. Nutno podotknout, že ani přijetí sebelepších protiopatření nemůže vyloučit negativní okolnosti, jakými jsou např. nedbalostní jednání, selhání lidského faktoru či poškození stop způsobené úmyslným jednáním.

3.1 Fáze vyhledávání digitálních stop

Fáze zajišťování a vyhledávání digitálních stop je úvodní fází práce forenzních IT specialistů a vyšetřovatelů, která na místě činu v rámci vyhledávání stop probíhá. Z tohoto důvodu je nezbytné počínat si při vyhledávání stop velmi obezřetně. Zejména v okamžiku, kdy jsou propátrávány rozsáhlejší a členité prostory, je velmi nutná koordinace celého týmu.

1) **Riziko nerozeznání digitální stopy**

Úvodem je třeba podotknout, že vyhledávání digitálních stop je disciplínou poměrně složitou. Nejen, že se digitální stopy mohou ukrývat na nejrůznějších místech, ale také mohou klamat svým vzhledem. V dnešní době je možno se setkat s nejrůznějšími podobami USB paměťových zařízení, které jsou k nerozeznání např. od šperku, dětské hračky či přívesku na klíče.

2) **Riziko přehlédnutí digitální stopy**

Na samotném místě činu je nezbytné věnovat zvláštní pozornost i znakům, které by mohly poukazovat na přítomnost zařízení, které mohlo být úmyslně skryto. Typickým příkladem může být např. NAS server ukrytý v technické místnosti objektu, ale i nahrávací zařízení v podobě dekorace umístěné na poličce v obývacím pokoji. V tomto případě je na místě přijetí takových opatření, která povedou k zajištění systematického postupu vyhledávání digitálních stop.

3) Riziko nedostatečné koordinace vyhledávání stop

Důležitá je nejen celková koordinace osob, které prohlídku provádějí, ale také určení jednotného postupu. Z teorie kriminalistické taktiky jasně vyplývá, že ohledání místa činu je možno provádět několika doporučenými způsoby. V odborné literatuře se hovoří např. o frontálním, koncentrickém či excentrickém způsobu provádění ohledání místa činu. V případě, že je jeden z možných způsobů zvolen, je třeba ho bez výhrady dodržovat. Jedině tak je možné dosáhnout kýženého výsledku.

3.2 Fáze zajišťování digitálních stop

V okamžiku kdy jsou veškeré digitální stopy vyhledány je na řadě realizovat jejich zajištění.

4) Riziko zajištění nekompletní stopy

V této fázi by na zajišťování stop měl vždy participovat specialista na příslušnou problematiku. V opačném případě, tedy kdyby zajištění stop bylo prováděno neodborně, či laicky, mohlo by dojít k jejich nevratnému poškození. Běžně tak může nastat situace, kdy dojde k chybné identifikaci stop, které je nezbytné zajistit, případně může dojít k situaci, kdy je stopa zajištěna nekompletní, a tudíž není možné následně provést její zkoumání.

5) Riziko neodborné manipulace se stopou

Jako etrémní se jeví situace, kdy dojde při provádění domovní prohlídky či prohlídky jiných prostor a pozemků k nálezu spuštěného počítače nebo podobného zařízení a toto zařízení je bez jakékoliv konzultace a provedení základních forenzních úkonů, které byly popsány v předchozích kapitolách, vypnuto a odesláno ke zkoumání znaleckému ústavu. Netřeba dodávat, že v krajním případě může být takto neodborně zajištěno zařízení, které je opatřeno přístupovým heslem a využívá aktivního šifrování celého disku (FDE). V tento okamžik můžeme s pravděpodobností limitně se blížící jistototě hovořit o tom, že došlo ke znehodnocení stopy a eliminaci možnosti jejího vytěžení.

6) Riziko záměny stopy

Vyhledání a korektní zajištění stopy je možno označit jako jednu ze zásadních činností, které je na místě probíhajícího úkonu třeba provést. Po provedení vyhledání a zajištění stopy následuje na místě realizace činnost, která má za úkol provést správné označení, zabalení a utentizaci zajištěných stop. V této fázi je zásadní, aby při manipulaci se stopami nedošlo k jejich záměně. Tedy, aby každá nalezená stopa, které je přiřazeno číslo stopy byla s tímto

číslem nafotografána a následně pod stejným číselným označením zapsána do protokolu o prohlídce místa činu. Jedině tak je možno zajistit, že nedojde k možnému procesnímu pochybení.

7) Riziko chybného zabalení stopy

Po nafocení stopy a následném zaprotokolování je zásadní, aby byla stopa řádně zabalena. Celému postupu balení stop je v této práci věnována samostatná podkapitola, proto není nezbytně nutné zde tento potup opakovat. Pouze zde bude připomenuto, že stopy musí být zajišťovány a následně baleny do speciálně určených bezpečnostních obalů, které ochrání stopu před neoprávněnou manipulací. V okamžiku, kdy by nedošlo k dodržení této zásady, a stopa by byla zabalena takovým způsobem, že by bylo při jejím transportu či později možno se stopou jakkoliv manipulovat, připojovat k ní jiná zařízení nebo s ní nakládat jiným způsobem, hrozilo by, že dojde k napadení věrohodnosti takto zajištěné stopy a důkazní materiály pořízené vytěžením této stopy nebudou soudem akceptovány. V krajním případě by mohlo dojít k vyloučení veškerých digitálních důkazů, které byly současně předloženy. Toto riziko je možno eliminovat pouze doržováním stanoveného postupu korektního zajišťování a balení stop a následné manipulace s nimi.

3.3 Fáze pořizování bitové kopie stopy

Vtvoření bitové kopie ze zajištěného zařízení patří mezi zásadní operace, které lze na místě, kde právě probíhají úkony v rámci trestního řízení provádět, a proto také na správnosti provedení bitové kopie závisí další postup, které jsou při práci digitálními stopamy prováděny.

8) Riziko zápisu dat na digitální stopu

Na prvním místě přichází v úvahu situace, která může nastat na počátku technologického postupu samotného pořizování bitové kopie stopy. Jedná se o situaci, která je ve vztahu k integritě stopy jednoznačně ohrožující. Uvažujme situaci, kdy je pořizována bitová kopie pevného disku za použití zajištěného počítače. V tento okamžik se nabízí možnost vzniku chyby v okamžiku, kdy je k počítači připojen technologický disk, do USB portu je zasunuto paměťové zařízení s „live“ distribucí forenzního systému, ale po zapnutí počítače dojde k nabootování ze zájmového disku. Jak již bylo několikrát řečeno, v tomto případě dochází k přepisu systémových informací o stavu počítače a takto znehodnocená stopa se stává prakticky nevyužitelnou a lehce napadnutelnou. V případě, kdy forenzní IT specialista

využívá svého technologického počítače, je možnost vzniku této chyby minimalizována v důsledku znalosti použitého počítače. V okamžiku, kdy se vyskytnou nějaké pochybnosti o nastavení bootovací sekvence na technologickém počítače, je možno provést kontrolní spuštění počítače bez připojeného zájmového disku a ověřit tak nastavení bootování z USB zařízení – tedy zavedení forenzní distribuce systému GNU/Linux.

9) Riziko chyby v syntaxi příkazu

Mnohem závažnější se poté jeví chyba, která může nastat z důvodu nepozornosti či nedbalosti. Při každé lidské činnosti hraje selhání lidského faktoru riziko, ktreré nelze stoprocentně eliminovat. Pro získání bitové kopie ze zajištěného média je využíváno postupů, kteé jsou prováděny v terminálu forenzního systému. Tento okamžik, kdy je prováděna práce v systémovém terinálu, můžeme z hlediska činnosti na místě domovní prohlídky či prohlídky jiných prostor považovat za kritický z hlediska nutnosti dodržení maximální koncentrace na práci. Velmi snadno totiž vylivem vyrušení může dojít při zadávání jednotlivých příkazů ke vzniku chyby v syntaxi příkazu, či k chybě ve formě zadaného parametru. V tomto okamžiku je riziko jediné – příkaz nebude akceptován a nedojde k jeho provedení, nebo bude proveden s jinými parametry. Toto pochybení má všech možná východiska řešení. V případě neprovedení příkazu nehrozí žádné poškození zajištěné stopy a příkaz je možno přepsat a provést opakovaně.

10) Riziko chyby v parametru příkazu

Ve situaci, kdy je příkaz vykonán s chybnými parametry, je možno tuto skutečnost akceptovat (například dojde k omylu při zadávání parametru „*split*“) a případně příkaz provést opakovaně s korektně nastavenými parametry příkazu. V ani jednom z předešlých případů nedojde k nevratnému znehodnocení stopy, a celý postup se může opakovat.

11) Riziko záměny zdrojového a cílového média

V případě kdyby došlo při zadávání příkazu „*dd*“ nebo jeho alternativ k tak fatálnímu selhání, jako je záměna zdrojového a cílového média, tedy k obrácení parametrů „*if=*“ a „*of=“*, znamenalo by to, že by došlo k zápisu bitové kopie technologického disku na disk zájmový. Takovéto selhání by poté vedlo k trvalému znehodnocení zajištěné stopy. Pro minimalizaci rizika, že dojde k chybnému zadání příkazu do systémové terminálu a následnému znehodnocení zajištěné stopy se nabízí zavedení vícestupňové kontroly zadaného příkazu – tedy správnost příkazu konzultovat s kolegou či znalcem, který je na místě úkonu přítomen, případně se nabízí možnost přistoupit při pořizování bitové kopie

k použití utility, kde probíhá nastavení parametrů v grafickém prostředí (např. dříve jmenovaná utilita Guymager) a vyhnout se tak zadávání parametrů ručně, tedy do příkazové řádky.

12) Riziko úmyslného znehodnocení stopy

Ke znehodnocení digitální stopy však nemusí nutně dojít pouze z důvodu nedbalosti či nepozornosti ze strany osoby, která zajišťování stop rovádí. Na tomto místě je třeba uvést, že zájem na zničení či znehodnocení digitálních stop mohou mít i jiné osoby, které se v průběhu provádění úkonů v rámci trestního řádu nacházejí na místě realizace zákroku. Takovouto osobou může být v prvé řadě osoba, která je dotčena probíhajícími úkony – tedy osoba pachatele či podezřelého. Ve druhé řadě se však může jednat i o osobu rodinného příslušníka, správce IT vybavení, nebo majitele společnosti, který může mít zájem na tom, aby došlo ke zničení či znehodnocnení digitálních důkazů. Je nutno podotknout, že na místě probíhajích úkonů se v žádném případě nesmí pohybovat nepovolané osoby, a osoby, které jsou na místě probíhajících úkonů přítomny by měly být pod neustálým dozorem tak, aby příležitost pro znehodnocení jakékoliv stopy, vůbec nevznikla. V prvé řadě je nezbytné dohlédnout, aby ze strany neautorizovaných osob nedocházelo nebo nedošlo v žádném případě k pokusu o manipulaci s jakýmkoliv zařízením, které by mohlo být digitální stopou. Osoby jako takové je třeba v průběhu probíhajících úkonů nepřetržitě střežit a nenechávat bez dozoru.

13) Riziko neoprávněné manipulace se stopou

V okamžiku, kdy jsou na místě realizace prováděny zálohy digitálních stop, je nepřípustné, aby probíhající zálohování bylo necháno bez dozoru. V optimálním případě by měl být celému procesu přítomen forenzní IT specialista či znalec. V případě, kdy je nezbytná činnost znalce na jiném místě v rámci probíhající domovní prohlídky nebo prohlídky jiných prostor, je z důvodu zabezpečení stopy doporučeno, aby byl proces zálohování střežen policistou. V situacích, kdy probíhá zálohování velkého množství dat (v řádu TB), tj. v okamžiku, kdy dochází k získávání dat např. ze serverového úložiště, a je zřejmé, že celý proces zálohování zabere několik hodin, nebo dokonce v extrémních případech i několik dní. Je vhodné na začátku zálohování zvolit pro celý proces takovou místnost, kterou je možno uzamknout a náležitě zabezpečit. V mnoha situacích těmto parametrům odpovídají právě místnosti serveroven, které jsou nepřetržitě střeženy proti neoprávněnému vniknutí v systému 24/7. Do místnosti serverovny poté může být umístěn technologický disk, který

se nejčastěji připojí na rozhraní samotného serveru nebo na rozhraní počítače, ze kterého je správa serveru realizována. Po spuštění zálohování je možno takovouto místnost uzamknout a zajistit proti neoprávněnému vniknutí. Toto opatření je zpravidla realizováno zapečetěním vstupních dveří do místnosti a ustanovením ostrahy, která bude vstup do místnosti střežit. Před každým návratem do místnosti je poté provedena kontrola neporušenosti pečeti.

3.4 Ostatní rizika při manipulaci s digitálními stopami

Výše uvedené podkapitoly pojednávaly o dvou zásadních fázích při samotném procesu zajišťování digitálních stop a při následné manipulaci s těmito stopami za účelem získání jejich bitové kopie.

14) Riziko odcizení digitální stopy

V rámci této podkapitoly je důležité upozornit na situaci, která může nastat nejen v rané fázi domovní prohlídky, tedy v okamžiku vyhledávání důkazů samotných, ale i v okamžiku, kdy jsou všechny stopy zajištěny, zabaleny a probíhají další úkony v rámci trestního řízení. Jedná se o situaci, kdy dojde z nějakého důvodu k odcizení či ztátě digitální stopy, či stop. Tento druh rizika je na místě v okamžiku, kdy jsou podceňována veškerá bezpečnostní opatření – tzn. že dojde k nekontrolovanému pohybu osob v prostorách, kde jsou stopy shromažďovány, jsou podceněna pravidla při převozu stop do prostor, které jsou určeny k jejich skladování, nebo jsou porušeny zásady manipulace se zajištěným materiálem. Zde se nabízí jediná možnost, jak tomuto zabránit. Bez výhrady doržovat veškerá bezpečnostní opatření, která se vztahují nejen k pohybu v místě, kde probíhají úkony v rámci trestního řízení, ale také doržovat pravidla, která se vztahují k práci se stopami. [4]

Příklad vhodného nastavení pravidel pro skladování digitálních stop:

- Veškerý zajištěný materiál je nutno po celou dobu skladovat na místech k tomu určených. Pro snížení rizika krádeže či manipulace se stopami opatřit toto místo dodatečným poplachovým zabezpečovacím zařízením.
- Při skladování stop využívat mimo jiné i prostředky předmětové ochrany, jako jsou ocelové skříně, trezory nebo trezorové místnosti. Těchto prostředků by mělo být využíváno i v okamžiku skladování bitových kopií a jejich záloh, které jsou uloženy na technologickém médiu.
- Bitové kopie neukládat na volně přístupná datová úložiště. I v případě, že se jedná o interní, metalicky oddělenou sít, je doporučeno, aby byly bitové kopie vždy

uloženy na zařízení, které je možno zajistit prostředky předmětové ochrany (např. osobní diskové pole). V případě, že jsou zálohy ukládány na společné úložiště (např. v rámci oddělení), nabízí se varianta ukládání záloh do adresářů, kdy je přístup do tohoto adresáře podmíněn autorizací uživatele.

- Jakoukoliv manipulaci s digitálními stopami, např. předání stop jiné osobě, je nutno provádět vždy po sepsání záznamu, ve ktrém budou uvedeny nacionále obou osob, určena zodpovědnost za přebraný materiál a dále zde bude definováno, jaké stopy byly předány.
- Zajištěné digitální stopy nenechávat za žádných okolností volně bez dozoru. V každé fázi, kdy je se stopami nakládáno zajistit jejich střežení proti neoprávněné manipulaci.

V praxi je možno definovat celou řadu rizik, která mohou při práci s digitálními stopami nastat. Ve výše uvedeném textu jistě nebyly uvedeny všechny možnosti, které mohou ohrozit integritu digitální stopy, přesto je nutné si uvědomit, že tato rizika jsou reálná, a v žádné fázi procesu nakládání se zajištěným materiálem nemohou být podceňována. V následující tabulce (Tab. 1) je shrnut výskyt jednotlivých rizik, která hrozí v konkrétních fázích zajišťování digitálních stop.

Tabulka 1. Pravděpodobnost výskytu rizika v jednotlivých fázích zajišťování digitálních stop (zdroj: vlastní)

	Nerozeznání DS	Přehlédnutí DS	Nedostatečná koordinace	Nekompletní zajištění DS	Neodborná manipulace	Záměna DS	Chybné zabalení DS	Zápis dat na DS	Chyba v syntaxi příkazu	Chyba v parametru příkazu	Záměna zdroje a cíle	Znehodnocení stopy	Neoprávněná manipulace	Odcizení DS
Fáze vyhledávání DS	X	X	X	X	X								X	X
Fáze zajišťování DS				X	X	X	X						X	X
Fáze pořizování bitové kopie					X			X	X	X	X	X	X	X

4 POROVNÁNÍ JEDNOTLIVÝCH METOD ZAJIŠŤOVÁNÍ DIGITÁLNÍCH STOP

V teoretické části této práce byly charakterizovány nejčastěji používané metody vhodné pro zajišťování digitálních stop na místě činu. Cílem této kapitoly je provést zhodnocení jednotlivých metod na základě zvolených hodnotících kritérií, která budou stanovena, a nalézt tak klíč pro volbu optimálního postupu pro zajištění digitálních stop nalézajcích se na místě činu. Vzhledem k úvaze, že ne všechny metody zajišťování stop jsou uplatnitelné napříč celým spektrem podob digitálních stop, je cílem této kapitoly také přinést přehled o tom, jaké postupy by měly být využity pro zajištění jednotlivých technických zařízení či dat, která mají charakter digitální stopy.

4.1 Stanovení kritérií pro volbu vhodné metody

Tato podkapitola definuje několik základních kritérií, která by měla být při práci na místě činu a před samotným započetím zajišťování digitálních stop rozhodující při prvnotní úvaze, jaká technologická zařízení budou použita pro vytváření záloh digitálních stop a jakým způsobem budou digitální stopy zajišťovány. Po zhodnocení všech faktorů by tak mělo dojít ke zvolení optimálního způsobu zajištění digitálních dat.

Jednotlivá kriteria byla zvolena následovně:

A. Komplexní zajištění stopy

Kriterium komplexního zajištění stopy může být chápáno jako jeden ze zásadních faktorů, které by měly hrát roli při zajišťování digitálních stop. Komplexní zajištění stopy je možno chápat jako takové zajištění stopy, které vede v následném procesu zkoumání k vytěžení maximálního možného objemu dat a informací.

B. Neporušení integrity stopy

Neporušení integrity stopy je možno chápat také ve smyslu neznehodnocení stopy. Toto kritetium má zajistit, aby byl na základě informací o charakteru místa realizace úkonů zvolen takový postup zajišťování digitálních dat, který bude vzhledem k druhu zajišťovaných stop nejvhodnější. Zjednodušeně se dá říci, že by měl být v závislosti na povaze místa, kde dochází k zajišťování digitálních stop, zvolen takový postup, který povede k minimalizaci možného selhání při zajišťování stop. Neporušit integritu stopy znamená např. zabránění nechtěnému zápisu na stopu během vytváření bitové kopie.

C. Technické nároky na zajištění stopy

Posouzení technických nároků na zajištění stopy je zásadní v okamžiku, kdy mají být zajištěna data ze zařízení, která např. nejsou sériově vyráběna, tedy z takových zařízení, která byla vyrobena pro potřeby plnění specializovaných automatizovaných kroků ve výrobě či průmyslu a k jejichž zajištění je zapotřebí specializované technické vybavení. Dále se může jednat o zařízení, ktrerá nejsou mezi populací běžně rozšířena a o zařízení, u kterých jsou aplikována opatření vedoucí ke znesnadnění přístupu bez potřebné autorizace (šifrování, přístupové heslo, atp.).

D. Časové nároky na zajištění stopy

Kriterium časové náročnosti by mělo být bráno v úvahu převážně v okamžiku, kdy jsou zajišťovány stopy, které svým charakterem vyžadují použití na čas náročného technologického postupu. Časová náročnost v mnoha případech souvisí i s nároky na specializované vybavení jak softwarové, tak hardwarové.

Aplikaci kritéria časové náročnosti můžeme uvažovat také v případě, kdy je nezbytné zajistit velké množství různorodých stop.

E. Datový objem zajišťovaných stop

Datový objem stop úzce souvisí s kritetiem časové náročnosti na zajištění stopy. Zjednodušeně se dá říci, že čím větší je objem dat zajišťovaných stop, tím větší jsou nároky na časovou dotaci potřebnou pro jejich zajištění.

Toto kriterium však může být aplikováno i v okamžiku, kdy objem dat, která jsou na místě realizace z jednotlivých digitálních stop zajišťována při vytváření bitových kopií převyšuje datovou kapacitu technologických disků. Ke zjištění informace o potřebné kapacitě technologických disků dochází až v okamžiku, kdy je zjištěn celkový objem zajišťovaných dat

F. Nároky na lidské zdroje

Potřeba zvážit kriterium náročnosti aplikace metody zajišťování digitálních stop na lidské zdroje přichází v okamžiku, kdy jsou zajišťována data ze zařízení takového charakteru, které si vyžaduje použití specifického pracovního postupu. K posouzení nároků na lidské zdroje by mělo dojít již na základě vyhodnocení operativní situace před samotným započetím zajišťování digitálních stop.

4.2 Hodnocení jednotlivých metod v závislosti na stanovených kritériích

V podkapitole 4.1. bylo stanoveno šest kritérií, která by měla být rozhodující při úvaze, jaká metoda zajištění digitálních stop by měla být zvolena, aby došlo k optimálnímu prolnutí všech definovaných kritérií a zároveň, aby bylo zajištění digitální stopy provedeno co nejčistším způsobem. Tedy, aby byla digitální stopa zajištěna korektně. V následujícím textu bude provedeno zhodnocení jednotlivých metod, které jsou využitelné pro zajišťování digitálních stop na základě jednotlivých kritérií, která byla výše stanovena.

4.2.1 Metoda zajištění stopy „in natura“

Zajištění stopy „in natura“ znamená, že je stopa zajištěna jako celek bez toho, aniž by s ní na místě realizace úkonů byly prováděny jakékoliv činnosti forenzního zkoumání. Stopa, která je takto zajištěna je pouze vyfotografována, zaprotokolována a vhodně zabalena a uložena k převezení na znalecké pracoviště či do laboratoře.

- **Kriterium A - komplexní zajištění stopy**

Při zajištění stopy „in natura“ je stopa zajištěna komplexně, jelikož je zajišťována jako jeden technologický celek a nedochází tak k zásahu do stopy na místě realizace úkonu. Následné zkoumání stopy je prováděno až na znaleckém pracovišti či v laboratoři a mohou se na něm podílet i znalci jiných odborností, což v některých případech může přispět k maximalizaci získaných dat a informací o stopě. V případě, že jsou stopy zajišťovány „in natura“ dá se hovořit o tom, že jsou zajištěny komplexně.

- **Kriterium B - neporušení integrity stopy**

V případě zajišťování digitálních stop na místě realizace úkonů trestního řízení je zásadní, aby nedošlo z žádného důvodu k porušení integrity stopy, které by mělo za následek její znehodnocení. Zajistit stopu „in natura“ může znamenat eliminaci rizika poškození integrity stopy na minimum, jelikož se stopou nejsou na místě úkonu prováděny žádné činnosti forenzního charakteru. Zajistit stopy „in natura“ může být doporučeno v okamžiku, kdy se jedná o zajišťování stop z v takovém prostředí, kde je zvýšené riziko vzniku chyby lidského faktoru. Tedy tam, kde jsou ztížené pracovní podmínky v důsledku stresu.

- **Kriterium C - technické nároky na zajištění stopy**

V tomto případě se jedná o absolutně technicky nenáročnou operaci, která nevyžaduje žádné specializované vybavení. Ve chvíli, kdy je rozhodnuto o tom, že bude stopa zajištěna „in natura“ je z hlediska potřeby technického vybavení tato činnost zanedbatelná.

- **Kriterium D - časové nároky na zajištění stopy**

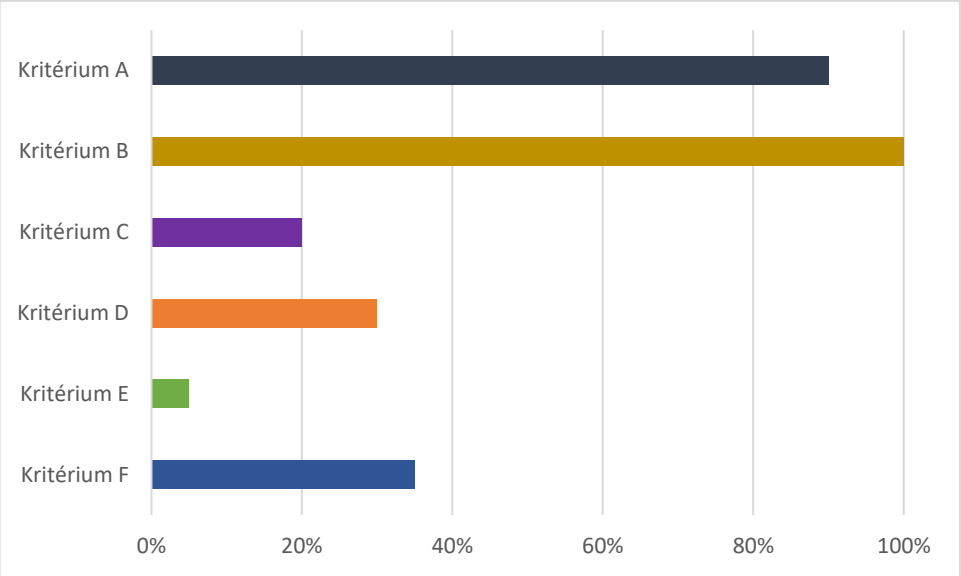
Časová náročnost při zajišťování stop „in natura“ je minimalizována. V okamžiku, kdy je rohodnuto o zajištění stopy tímto způsobem, spočívá časové zatížení pouze v případě, kdy je zapotřebí stopu korektně zajistit – to může znamenat např. činnost, při které dochází k demontáži stopy (odpojení konektivity)

- **Kriterium E - datový objem zajišťovaných stop**

Kritetium datového objemu je v tomto případě možno zcela zanedbat. Vybrané stopy, které budou zajišťovány, jsou převezeny na znalecké pracoviště či do laboratoře, která by měla disponovat dostatečnou kapacitou volného prostoru pro ukládání zájmových dat. Na znaleckých pracovištích je toto řešeno převážně oddělenými serverovými úložišti s kapacitou převyšující několik desítek TB, která jsou určena pro uchovávání zajištěných dat.

- **Kriterium F - nároky na lidské zdroje**

Stejně, jako kriterium datového objemu, se jeví v okamžiku, kdy jsou stopy zajišťovány „in natura“ kriterium lidských zdrojů zcela zanedbatelně. Ne vždy tomu tak musí být. V případě, kdy je rozhodnuto o zajištění stop „in natura“ a dochází k zajišťování např. běžné kancelářské výpočetní techniky, není pro tuto činnost zapotřebí kooperace speciálně vyškolených odborníků. Může však nastat situace, kdy bude zapotřebí zajistit např. avioniku z havarovaného letounu, a v takovémto případě se bez osoby znalé této problematiky na místě činu prakticky neobejdeme.



Obrázek 1. Grafické znázornění vhodnosti metody zajištění stop „in natura“ s ohledem na volbu jednotlivých kriterií (zdroj: vlastní)

4.2.2 Metoda zajištění stopy pomocí jednoúčelového technického zařízení

Použití jednoúčelového technického zařízení pro zajištění digitální stopy znamená, že je pro tento účel použito takového zařízení, které bylo k dané činnosti speciálně vyrobeno či upraveno. Blíže je tato problematika rozebrána ve výše uvedené kapitole č. 2.

- **Kriterium A - komplexní zajištění stopy**

Použitím jednoúčelového technologického zařízení pro zajištění digitální stopy je chápáno použití zařízení na duplikaci disků nebo speciálně upraveného technologického počítače. V případě, že jsou tato zařízení použita v souladu s dodržením technologického postupu je zaručeno, že stopa bude zajištěna komplexně, a bude tak možné se stopou i nadále pracovat. Tato zařízení jsou určena k pořízení bitové kopie obsahu celé logické i fyzické paměti zařízení. Na takto zajištěné stopě lze následně provádět komplexní znalecké zkoumání, které může zahrnovat i zkoumání smazaných dat z nealokovaného prostoru disku.

- **Kriterium B - neporušení integrity stopy**

Při zajišťování dat pomocí jednoúčelového technologického zařízení je nutné brát v úvahu, že za určitých okolností může dojít k porušení integrity stopy. Vzhledem k tomu, že jsou tato zařízení obsluhována člověkem, není zcela vyloučena možnost selhání lidského faktoru, ke kterému může za určitých okolností dojít. Rizikové jsou především okamžiky, kdy je toto zařízení použito ve stížených pracovních podmínkách. Selháním lidského faktoru poté může

dojít k pokškození stopy. Proto je nutné zvážit i možná rizika, která ohrožují digitální stopu při práci s tímto druhem zařízení. Pro ilustraci je možno uvést v krajním případě např. záměnu zdrojového a cílového média.

- **Kritetium C - technické nároky na zajištění stopy**

Metoda zajištění stopy jednoúčelovým technickým zařízením klade zvýšené nároky na použité technické zařízení. V případě, kdy dochází k zajišťování dat z disků počítačů, externích disků či USB paměťových médií, vystačí si forenzní IT specialista s upraveným technologickým počítačem, který je pro tuto činnost určen. Je-li zapotřebí provést na místě realizace zálohu mobilních telefonů, tabletů, nebo jiné komunikační techniky, je zapotřebí přítomnost specializovaného HW zařízení, které je určeno pro získávání dat z tohoto druhu techniky (např. zařízení UFED)

- **Kriterium D - časové nároky na zajištění stopy**

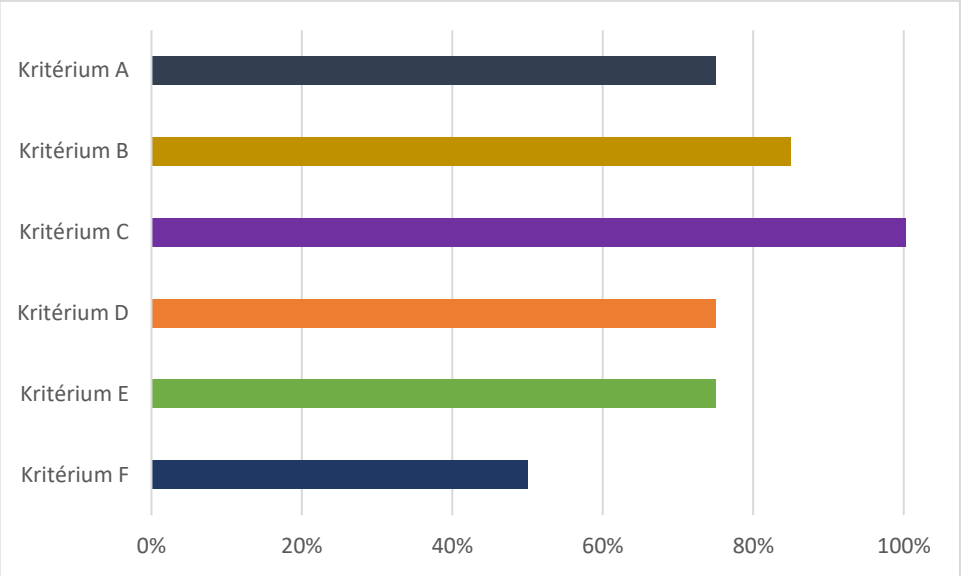
Zajištění dat na místě, kde probíhají úkony v rámci trestního řízení si klade zvýšené nároky na potřebnou časovou dotaci. Zde hraje svou roli několik faktorů, a proto je nezbytné posoudit, zda je nutné provádět zajištění bitových kopií digitálních stop v plném rozsahu na místě realizace. Tzn. vyhodnotit, které stopy je nezbytné zajistit na místě, a které mohou být zajištěny „in natura“ a převezeny ke zkoumání na znalecké pracoviště. Takovéto úvahy jsou na místě v okamžiku, kdy je potřebné zajistit data z širokého spektra různých zařízení.

- **Kriterium E - datový objem zajišťovaných stop**

Při zajišťování digitálních stop za pomoci jednoúčelového technologického zařízení je zapotřebí zhodnotit, zda je na místě zákroku k dispozici dostatečné množství technologických disků s potřebnou kapacitou. Datový objem zajišťovaných stop také souvisí s časovými nároky, které jsou rostoucí s objemem zajišťovaných dat.

- **Kriterium F - nároky na lidské zdroje**

Použití jednoúčelového technologického zařízení pro zajištění digitálních stop si neklade zvýšené nároky nalidské zdroje. V okamžiku, kdyje použito zařízení pro duplikování disků, je vytvoření bitové kopie poměrně nenáročnou činností, jelikož se jedná o zařízení, které je k tomuto účelu speciálně vyrobeno a menu přístroje vede jeho obsluhu prakticky krok za krokem.



Obrázek 2. Grafické znázornění vhodnosti metody zajištění stop pomocí jednoúčelového technického zařízení s ohledem na volbu jednotlivých kriterií (zdroj: vlastní)

4.2.3 Metoda zajištění stopy pomocí zkoumaného systému

Zajišťování stop pomocí zkoumaného systému spočívá ve využití zajištěného zařízení, ke kterému je následně připojen technologický disk a po zavedení operačního systému GNU/Linux jsou z tohoto zařízení následně vykopírována zájmová data, resp. Je vytvořena bitová kopie pevného disku zařízení. K využití zkoumaného systému pro zajištění dat přistupujeme v okamžiku, kdy např. není možné ze zařízení vyjmout pevný disk bez složité demontáže (zařízení typu All in One) či na místě realizace není k dispozici jednoúčelové technické zařízení pro pořízení bitové kopie zájmového disku.

- **Kriterium A - komplexní zajištění stopy**

Zajištění stopy pomocí zkoumaného systému je z hlediska komplexního zajištění stopy srovnatelné s použitím jednoúčelového technického zařízení. I v tomto případě dochází k vytvoření kompletní bitové kopie disku, a tím pádem je umožněno následné komplexní zkoumání na znaleckém pracovišti či v laboratoři.

- **Kriterium B - neporušení integrity stopy**

V okamžiku, kdy je stopa zajišťována pomocí zkoumaného systému, je třeba pamatovat na možnost porušení integrity stopy. Zde přichází v úvahu situace, kdy znalec pracuje se zařízením, které nezná, a může tak nastat nastat problém, kdy při zpuštění počítače nedojde

k zavedení „live“ distribuce systému GNU/Linux, ale je zaveden operační systém ze zájmového média. V tento okamžik dojde k jednoznačnému porušení integrity stopy.

- **Kriterium C - technické nároky na zajištění stopy**

V případě, že je k zajištění dat použito zkoumaného systému, nejsou kladeny na technické požadavky žádné zvláštní nároky. Jediné, co je za potřebí, je mít k dispozici USB disk s „live“ distribucí systému GNU/Linux a také je zapotřebí disponovat technologickým diskem s potřebnou kapacitou. K připojení technologického disku lze využít běžně dostupné USB to SATA redukce, případně dokovací stanice, která je k zájmovému počítači připojena.

- **Kriterium D - časové nároky na zajištění stopy**

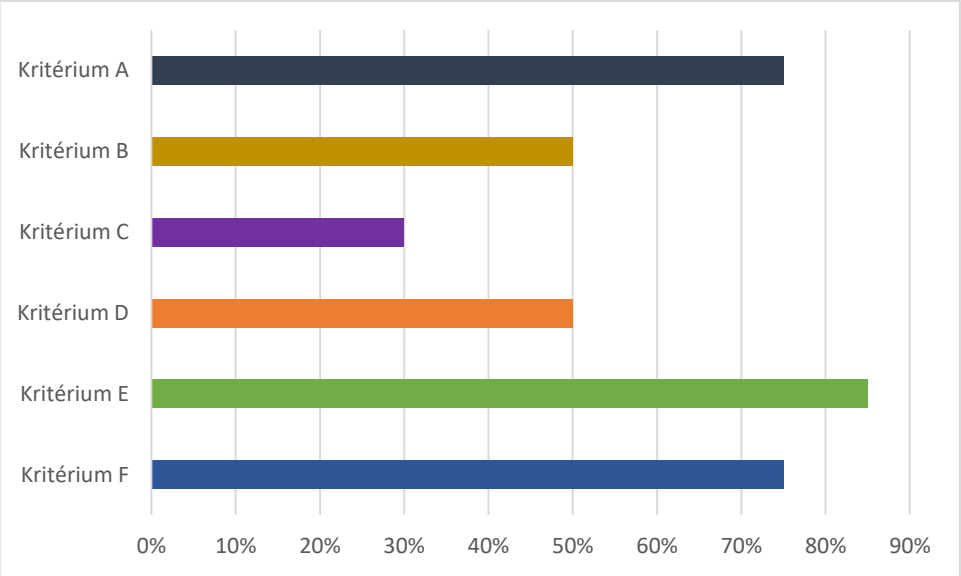
Pro časovou náročnost zajištění stop pomocí zkoumaného systému platí stejná pravidla, jako v případě použití jednoúčelového technického zařízení. Jediný argument, který je třeba brát v úvahu je skutečnost, že je pracováno se zařízením neznámým, a tudíž může dojít k prodloužení času potřebného k vytvoření bitové kopie. Takováto zařízení mohou být také různé konfigurace, a proto bude pro stanovení časové náročnosti postupu rozhodující i tento faktor. Poslední argument, který může ovlivnit potřebnou časovou dotaci je skutečnost, že je zkoumáno nestandardní zařízení, tedy takové zařízení, které bylo vyvinuto k nějakému specializovanému účelu, např. CNC obráběcí stroj.

- **Kriterium E - datový objem zajišťovaných stop**

Datový objem zajišťovaných stop souvisí s potřebou dostatečné kapaicty technologických disků na místě prováděného úkonu. Platí zde prakticky totéž, jako když je k zajištění dat použito jednoúčelového technického zařízení.

- **Kriterium F - nároky na lidské zdroje**

Nároky na lidské zdroje jsou v tomto případě v porovnání s předchozí metodou zajišťování stop neporovnatelné. V okamžiku, kdy jsou získávána data pomocí zajištěného systému, je nezbytné, aby zajišťování těchto dat prováděl znalec, nebo, aby byl znalec těmto úkonům alespoň přítomen jako odborný konzultant.



Obrázek 3. Grafické znázornění vhodnosti metody zajištění stop pomocí zkoumaného systému s ohledem na volbu jednotlivých kriterií (zdroj: vlastní)

4.2.4 Metoda zajištění stopy ze živého zkoumaného systému

Zajištění dat ze živého zkoumaného systému se rozumí situace, kdy je na místě činu nalezen zapnutý počítač, či jiné zařízení, které je v provozu, a jeho vypnutím by hrozila ztráta některých důležitých informací nebo dat. Jedná se o postup, který je co do potřebné odbornosti obsluhy velmi náročný. Data, která jsou zajišťována na živém systému, jsou ve veětšině případů kopírována na technologický disk, ale mohou být také zaznamenávána např, fotograficky. K tomuto způsobu zajištění dat může dojít v případě, kdy zařízení neobsahuje žádné rozhraní, pomocí kterého by mohlo být připojeno technologické médium.

- **Kriterium A - komplexní zajištění stopy**

Zajišťováním dat ze živého zkoumaného systému je možno zajistit více údajů než v případě, kdy je pracováno se systémem ve vypnutém stavu. V okamžiku, kdy je systém zapnut, je možné provést před samotným pořízením bitové kopie pevného disku také zálohu RAM paměti spuštěného zařízení, která může obsahovat přístupová hesla a šifrovací klíče.

- **Kriterium B - neporušení integrity stopy**

Zásahem do živého, nebo-li spuštěného systému dochází k částečnému narušení jeho integrity. Každá operace, která je na živém systému prováděna, by měla být dělána s maximální opatrností tak, aby nědošlo k nechtěné manipulaci se soubory.

- **Kriterium C - technické nároky na zajištění stopy**

Práce na zajištěném živém systému nepředstavuje z hlediska nároků na potřebné technické vybavení nikterak zatěžující činnost. Pro pořízení bitové kopie ze zapnutého systému postačí USB paměťové médium, na kterém se nachází některý z preferovaných SW nástrojů, pro pořizování záloh na spuštěném systému (např. FTK Imager) a dále je zapotřebí disponovat USB to SATA redukcí nebo dokovací stanicí pro připojení technologického disku.

- **Kriterium D - časové nároky na zajištění stopy**

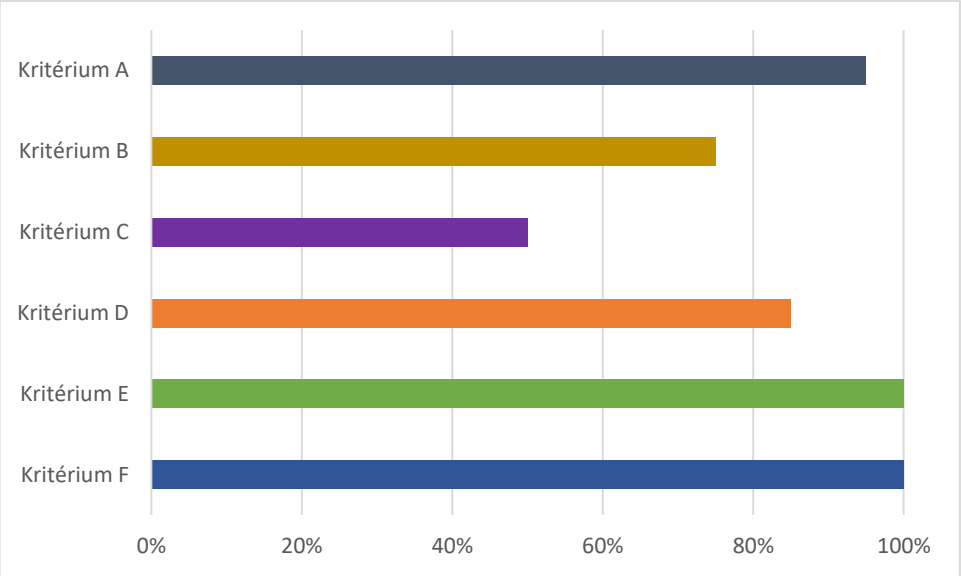
Časová náročnost při zajišťování dat ze živých systémů může být ovlivněna v případě, kdy je zapotřebí zajistit velké množství dat. Se spuštěným systémem pracujeme převážně v okamžiku, kdy jsou získávána data ze serverů, které ve většině případů slouží jako velkokapacitní úložiště. Na časovou náročnost má také vliv konektivita, která je využita pro připojení technologického disku, na který jsou data zálohována.

- **Kriterium E - datový objem zajišťovaných stop**

Datový objem zajišťovaných stop úzce souvisí s časovou náročností. V okamžiku, kdy jsou zajištována data z běžného kancelářského počítače, ktrerý obsahuje jeden pevný disk o kapacitě 500GB, je provedení zálohy poměrně nenáročné na dostupnou kapacitu technologického disku. Může však nastat situace, kdy jsou zajišťována data ze serveru, který slouží podniku o několika stovkách zaměstnanců, a v takovémto případě je potřebnou datovou kapacitu možno počítat v řádech desítek TB.

- **Kriterium F - nároky na lidské zdroje**

Zajištění dat ze živého systému je možno řadit mezi činnosti, které kladou vysoké nároky na lidské zdroje. Nejen, že by osoba, která zasahuje do živého systému měla být řádně proškolena, ale tato osoba by neměla postrádat ani dostatečné zkušenosti a znalosti, které jsou potřeba pro práci s neznámým systému. Je potřeba si uvědomit, že v případě, kdy budou zajišťována data z počítače, ne vždy se musí být v tomto počítači nainstalován operační systém MS Windows, se kterým většina uživatelů pracuje. V extrémním případě může být nezbytné zajistit data ze spuštěného technologického zařízení, jehož menu bylo naprogramováno pro jeden konkrétní účel. V takovémto případě se zřejmě neobjdeme bez pomoci odborníka z dodavatelské společnosti.



Obrázek 4. Grafické znázornění vhodnosti metody zajištění stop ze živého zkoumaného systému s ohledem na volbu jednotlivých kriterií (zdroj: vlastní)

4.3 Posouzení vhodnosti použití jednotlivých metod v závislosti na charakteru digitální stopy

Ve výše uvedeném textu bylo provedeno ohodnocení jednotlivých kritérií, a nastínění možných situací, které mohou být rozhodné při volbě metody, která bude použita pro zajištění digitálních stop. V následujícím textu jsou uvedena jednotlivá technologická zařízení, která se mohou na místě činu vyskytovat, a na základě předešlého hodnocení jednotlivých metod jsou u každého zařízení uvedeny argumenty, které by měly být brány v potaz v případě, kdy je rozhodováno, jaká metoda zajištění stopy bude použita.

4.3.1 Osobní stolní počítače – desktop

Potřeba zajištění dat z osobních stolních počítačů je v rámci provádění úkonů trestního řízení a v rámci potřeb následné forenzní analýzy jednou z nejčastějších činností, která může být na místě činu prováděna. Samotné počítače se mohou na místě činu nacházet v různém stavu (vypnuté / zapnuté) a dle toho, v jakém stavu je počítač nalezen, je také vhodné zvolit metodu, pomocí které budou data z počítače zajištěna.

Počítač je nalezen ve stavu:

A) **Vypnutý:** Při nálezu počítače ve vypnutém stavu je možné zvolit metodu jeho zajištění „in natura“, tedy počítač zajistit jako celek a následně transportovat

k dalšímu zkoumání na forenzní pracoviště. Případně je možné provést demontáž pevného disku počítače a za použití jednoúčelového technického zařízení provést pořízení bitové kopie na místě probíhajících úkonů trestního řízení.

B) **Zapnutý:** U počítače, který je nalezen v zapnutém stavu je vhodné aplikovat postup zajištění dat ze živého zkoumaného systému a provést tak nejen vytvoření bitové kopie disku zájmového zařízení, ale zajistit i kopii RAM paměti. V úvahu připadá i varianta, kdy po získání otisku paměti RAM je počítač vypnut a následně je pořízena bitová kopie pevného disku.

4.3.2 Osobní počítače typu notebook

Při zajišťování dat z notebooků, které se nacházejí na místě probíhajících úkonů trestního řízení je možno aplikovat stejný postup, který byl uveden v případě nálezu stolního osobního počítače. Technologický postup, kterým bude získána bitová kopie tohoto zařízení, volíme podle toho, zda se počítač nachází v zapnutém či vypnutém stavu. V případě, že je nalezený počítač vypnutý, zajišťujeme jen „in natura“, případně pro zajištění dat použijeme jednoúčelového technického zařízení. U počítače, který je nalezen v zapnutém stavu je v první řadě proveden otisk RAM paměti a následně je postupováno stejně, jako při zajišťování dat ze stolního počítače.

4.3.3 Osobní počítače typu netbook nebo ultrabook

Osobní počítače, které jsou označovány jako netbook a ultrabook jsou specifickou kategorií počítačů, jelikož pro jejich kompaktní rozměry, není velmi často možné provést demontáž pevného disku z těla zařízení, případně se jedná o tak specifické výrobky (např. MacBook), u kterých je provedení zálohy pevného disku na místě činu technologicky náročné, a proto je vhodné takováto zařízení zajišťovat převážně metodou „in natura“. Hlavní rozhodovací kritérium pro to, jak budou data z počítače zajištěna by mělo opět hrát to, v jakém stavu je zařízení nalezeno, a zda je možné provést na místě nálezu alespoň zálohu RAM paměti.

Zařízení je nalezeno:

A) **Zapnuté:** V tomto případě je vhodné pokusit se o zálohu RAM paměti a v případě, že to konstrukce zařízení dovoluje, provést zajištění bitové kopie na zapnutém systému. Po vytvoření zálohy RAM paměti je také možné počítač vypnout a následně demontovat pevný disk, který bude zálohován na technologické počítači.

B) **Vypnuté:** U vypnutého zařízení přichází v úvahu zajištění přístroje metodou „in natura“ nebo, pokud to konstrukce zařízení dovolí, provést demontáž pevného disku a tendo disk zálohovat omocí technologického počítače. Bitová kopie zájmového disku je poté uložena na technologické médium.

4.3.4 Servery

Zajišťování dat ze serverů je poměrně specifickou disciplínou, kdy ve valné většině případů dochází k pořizování záloh zájmových dat na spuštěném systému prostřednictvím speciálního administačního rozhraní. Z tohoto důvodu je také volena ta varianta zajišťování stop, kdy je k serveru připojen technologický disk, na který jsou zájmová data postupně vykopírována, případně je na tento technologický disk uložena bitová kopie. Může však nastat i situace, kdy je pro závažnost páchané trestné činnosti rozhodnuto, že dojde k zajištění celého serveru. Nelze vyloučit ani situaci, kdy je server nalezen ve vupnutém stavu, v takovém případě je na pečlivém uvážení, zda zařízení zajistit „in natura“, nebo zda ze serveru vymontovat pevné disky a provést jejich zálohu. V případě prvním může být server takových rozměrů, že nebude možné ho fyzicky transportovat. V případě druhém budou disky v serveru v tzv. RAID poli a získaná data z jednotlivých disků budou prakticky bezcenná.

4.3.5 Média pro uchování a přenos dat – CD/DVD

Jednotlivá nalezená média, která slouží pro nepřepisovatelné uchování a záznam dat, je vhodné zajistit metodou „in natura“. Pořizování kopií jednotlivých dicků na místě činu se z časové náročnosti jeví jako velice zdlouhavé. Navíc data, která jsou na disku uložena v nepřepisovatelné podobě jsou jen velmi obtížně manipulovatelná. Proto je často přistupováno k tomu, že takto nalezená média jsou označena, vyfotografována a po jejich zapsání do protokolu odvezena na znalecké pracoviště k jejich dalšímu zkoumání.

4.3.6 Externí disky

Nalezené externí disky, které se nacházejí na místě činu, je možno zajistit „in natura“ a po provedení všech úkonů, které souvisí se správným zajištěním stopy tyto disky odeslat ke zkoumání na znalecké pracoviště. Zde je třeba upozornit, že v průběhu celého procesu je třeba vést velmi důkladnou dokumentaci toho, jak je se zajištěnými externími disky nakládáno. Potřeba dokumentace postupu souvisí s možností úmyslného poškození integrity dat na takto zajištěném zařízení. Jako výhodnější se z tohoto hlediska jeví varianta, kdy je

na místě realizace provedeno vytvoření bitové kopie disku pomocí technologického počítače, či jednoúčelového technického zařízení, kdy je tato kopie opatřena kontrolní sumou, pro možnost kontroly integrity zajištěných dat. Vytvořená bitová kopie je uložena na technologické médium a následně odeslána ke zkoumání na znalecké pracoviště.

4.3.7 USB paměťová zařízení

Při zajišťování USB paměťových zařízení platí identická pravidla, jaká byla uvedena v podkapitole pojednávající o zajišťování dat z externích disků.

USB paměťová zařízení je možno zajistit:

- **A)** „in natura“
- **B)** Provedením bitové kopie pomocí technologického PC na místě realizace

4.3.8 Paměťové karty – SD, microSD, apod.

Při zajišťování paměťových karet platí identická pravidla, jaká byla uvedena v podkapitole pojednávající o zajišťování dat z externích disků. Zde je nutné uvést, že v případě zajišťování paměťovýh karet, které jsou součástí nějakého zařízení (např. diktafon, fotoaparát, kapesní scanner), je vhodné karty zajistit společně se zařízením, ve kterém jsou umístěny. Z tohoto důvodu je preferováno zajistit paměťové karty tzv. „in natura“

Paměťové karty je možno zajistit:

- **A)** „in natura“ (preferováno)
- **B)** Provedením bitové kopie pomocí technologického PC na místě realizace

4.3.9 Mobilní telefony

Mobilní telefony patří mezi zařízení, jejichž zajišťování se stalo prakticky samostatnou disciplínou v rámci provádění forenzních činností. Mobilní telefony se na místě činu mohou nacházet opět ve dvou stavech, tedy vypnuté a zapnuté. Ve většině případů jsou zajišťovány „in natura“ a jejich další zkoumání je prováděno na půdě znaleckého pracoviště. Může nastat i situace, kdy je záloha zajištěného mobilního telefonu provedena na místě realizace. V takovémto případě je pro zálohování dat použito jednoúčelové technické zařízení, např. zařízení UFED.

Mobilní telefon je nalezen ve stavu:

A) **Zapnutý:** U zapnutého zařízení je v první fázi aktivován tzv. režim letadlo, který je dnes obsažen v menu prakticky každého chytrého telefonu. Režim letadlo slouží k odpojení telefonu od konektivity. Zapnuté zaízení může být dále připojeno k technologickému počítači a pomocí speciálně určených forenzních nástrojů je provedena jeho záloha. V případě, že zálohu telefonu nelze na místě provést, mělo by dojít před vypnutím telefonu k deaktivaci bezpečnostních prvků, jakými jsou kód PIN nebo gesta pro odemčení obrazovky telefonu.

B) **Vypnutý:** Vypnutý mobilní telefon je zajištěn „in natura“ a předán k dalšímu zkoumání na znalecké pracoviště. Telefon, který je nalezen ve vypnutém stavu, musí být zkontrolován, zda neobsahuje kartu SIM, případně paměťovou kartu. Toto vše musí být uvedeno do protokolu a nafotografováno.

4.3.10 SIM karty

Při nalezení samostatné SIM karty na místě, kde jsou prováděny úkony v rámci trestního řízení je ve většině případů vhodné provést zajištění této stopy metodou „in natura“ a zajištěnou SIM kartu následně odeslat ke zkoumání na znalecké pracoviště. Na tomto pracovišti je poté provedena duplikace SIM karty a duplikát je následně podroben znaleckému zkoumání, kdy jsou ze zajištěné stopy vykopírovány veškeré uložené údaje. Často jsou takto zajištěny uložené SMS zprávy nebo telefonní čísla uložená na SIM kartě.

4.3.11 Tablety a PDA

Pro nalezené tablety a PDA platí stejná pravidla jako pro zajišťování mobilních telefonů. Při nálezu takovýchto zařízení je tedy doporučeno uvést toto zařízení do režimu letadlo a pokusit se na místě nálezu, a dokud je zařízení zapnuté o získání maximálního množství zájmových dat. Zejména jsou důležité údaje o uživateli, o uložených heslech a také informace, které jsou obsaženy v nainstalovaných chatovacích aplikacích a messengerech. Postup zajištění tabletů a PDA je v prováděných krocích identický s postupem, který byl specifikován u podkapitoly pojednávající o zajišťování dat z mobilních telefonů.

4.3.12 Aktivní síťové prvky – routery, firewally

Jedná se o specifická zařízení, která ve většině případů obsahují zájmové informace pouze v zapnutém stavu, proto je na prvním místě volen postup, kdy je zařízení analyzováno na místě nálezu, většinou za pomoci počítače, který je určen k administarci těchto zařízení. U

aktivních síťových prvků přichází v úvahu volba metody zajištění dat ze na živém systému. Jedná-li se o specifická zařízení, je přistoupeno k jejich zajištění metodou „in natura“.

4.3.13 Tiskárny a jiná reprodukční zařízení

Tiskárny a jiná reprodukční zařízení jsou zajišťována zejména v okamžiku, kdy dochází k páchání padělání cenin a tiskopisů. Vzhledem k tomu, že je zapotřebí provedení komplexního zkoumání více znaleckými odbornostmi (např. provedení grafické analýzy, chemické složení inkoustu), jsou tato zařízení zajišťována jako celek, tedy je využito metody „in natura“. Není ovšem vyloučeno, že bude zapotřebí provést zálohu paměti zapnutého zařízení, v takovémto případě je možno aplikovat i metodu zálohy na živém zkoumaném systému.

Tiskárna je nalezena ve stavu:

A) **Vypnuto**: Je-li nalezena tiskárna, nebo reprodukční zařízení ve vypnutém stavu, je z důvodu nutnosti podrobení tohoto zařízení komplexnímu zkoumání, zajištěno metodou „in natura“ a převezeno na znalecké pracoviště.
B) **Zapnuto:** U nálezu zapnutého zařízení je proveden pokus o zálohu paměti zařízení, která může obsahovat např. seznam naposledy tisknutých dokumentů, nebo jiné provozní a technické údaje, které byly zadány jejím uživatelem. Teprve po provedení zálohy paměti je toto zařízení vypnuto a následně zajištěno a odesláno k dalšímu zkoumání.

U zajištěných tiskáren a reprodukčních zařízení je ve většině případů stěžejní provedení jiných druhů zkoumání, jakými jsou např. grafická analýza tisku, pomocí kterého je možno provést srovnání grafické podoby zajištěných padělků a zkušebního tisku ze zajištěné tiskárny.

4.3.14 Skimmovací zařízení bankomatů

Jedná se o specifickou skupinu zařízení, která mohou být zajištěna na místě činu. Ve většině případů jsou tato zařízení zajištěna přímo na bankomatech. Málokdy jsou nalézána v rámci provádění úkonů trestního řízení (domovní prohlídky, apod.). Tato zařízení jsou zajišťována výhradně „in natura“ a po odeslání ke zkoumání znaleckému pracovišti jsou podrobena analýzám, na kterých se podílí více znaleckých odborností. U skimmovacích zařízení dochází velmi často k nálezu paměťových karet, na které jsou ukládány záběry z mikrokamery, která je součástí instalovaného zařízení.

4.3.15 Plastové karty s magnetickým proužkem

Plastové karty s magnetickým proužkem jsou často zajištěny v případech páchání majetkové trestné činnosti, a vzhledem ke specifickým postupům, které jsou aplikovány pro jejich zkoumání, jsou zajišťovány na místě realizace výhradně „in natura“ a následně odeslány ke zkoumání na znalecké pracoviště, kde jsou karty podrobeny důkladné analýze.

4.3.16 Nahrávací zařízení CCTV typu NVR, DVR

Záznamová zařízení, která jsou využita nejčastěji pro nahrávání sekvencí z kamer uzavřených televizních okruhů (CCTV) je nezbytné zajišťovat na místě nálezu vždy jako celek, případně provést vykopírování zájmových souborů na zapnutém systému. Je důležité upozornit na to, že zajištění pouze samotného pevného disku z nahrávacího zařízení je rovno zajištění stopy, která je pro další analýzu prakticky bezcenná. Většina nahrávacích zařízení je specifická v tom ohledu, že pro ukládání dat na pevný disk nepoužívají klasickou strukturu, kterou nacházíme u souborových systémů NTFS nebo FAT32. Tato záznamová zařízení využívají pevný disk podobně, jako když je prováděn záznam na magnetickou pásku. Z tohoto důvodu je nutné, pokud je rozhodnuto o zajištění nahrávacího zařízení, aby bylo zajištěno jako celek. Zejména z toho důvodu, že každý výrobce záznamových zařízení využívá jiné metody zápisu dat na pevný disk.

Metodu zajištění dat ze zařízení NVR nebo DVR tedy volíme podle toho zda je zařízení:

A) **Zapnuté:** Pokud to technické a časové možnosti dovolí, provedeme vykopírování souborů na živém, spuštěném zařízení. Pro vykopírování je využit technologický pevný disk.
B) **Vypnuté:** Zařízení zajišťujeme výhradně jako celek, tedy „in natura“.

4.3.17 Špionážní technika

Zařízení, která patří do kategorie špionážní techniky jsou ve většině případů specifická zařízení, jejichž zkoumání vyžaduje dostatečné technologické vybavení a zároveň zde může být žádoucí, aby tato zařízení byla zkoumána více znaleckými odbornostmi. Z tohoto důvodu je doporučeno zajišťovat prostředky špionážní techniky jako celek.

Tabulka 2. Sumarizace vhodných metod pro zajišťování jednotlivých drůhů zájmové techniky (zdroj: vlastní)

	„in natura“	jednoúčelové technologické zařízení	zkoumaný systém	živý zkoumaný systém
Osobní stolní počítače – desktop	X	X	X	X
Osobní počítače typu notebook	X	X	X	X
Osobní počítače typu netbook nebo ultrabook	X			X
Servery				X
Média pro uchování a přenos dat – CD/DVD	X			
Externí disky	X	X		
USB paměťová zařízení	X	X		
Paměťové karty – SD, microSD, apod.	X	X		
Mobilní telefony	X	X		X
SIM karty	X			
Tablety a PDA	X	X		X
Aktivní síťové prvky – routery, firewally	X			X
Tiskárny a jiná reprodukční zařízení	X			X
Skimmovací zařízení bankomatů	X			
Plastové karty s magnetickým proužkem	X			
Nahrávací zařízení CCTV typu NVR, DVR	X			X
Špionážní technika	X			

5 TECHNOLOGICKÝ POSTUP PRO ZAJIŠŤOVÁNÍ DIGITÁLNÍCH STOP NA MÍSTĚ ČINU

Obsahem této kapitoly je formulace obecného postupu, který by měl být použit při zajišťování digitálních stop na místě činu tak, aby byla minimalizována veškerá rizika, která mohou hrozit při zajišťování digitálních stop. Současně by aplikace níže uvedených doporučení měla vést ke zvýšení efektivity práce na místě činu a k zajištění všech stop, které se na tomto místě nacházejí tak, aby bylo možno provést jejich následné zkoumání v co nejširší míře a s využitím veškerých dostupných možností.

5.1 Vyhledávání digitálních stop

Vyhledávání digitálních stop je úvodní fází činností, které na místě realizace úkonů trestního řízení provádí skupina forenzních specialistů za účelem identifikace a odhalení veškerých zařízení, která mohou být považována z hlediska svých technických parametrů za digitální stopy, využitelné pro potřeby objasňování trestní věci.

Vyhledávání jednotlivých objektů zkoumání spočívá převážně v:

a) **Prokázání přítomnosti hardwarových komponent digitální techniky** – vyhledání veškerého hardwarového zařízení na místě činu hraje zásadní roli v okamžiku, kdy je nutné posoudit, zda byl s daným počítačovým systémem trestný čin spáchán.
b) **Prokázání výskytu informací určitého druhu na paměťových médiích** – tato činnost souvisí se zajištěním veškerých informací, které mohou mít vypovídající hodnotu o průběhu spáchaného trestného činu, případně informací, které mohou přinést rozhodující údaje o práci s daty, která jsou na paměťových médiích uložena.

Při vyhledávání digitálních stop je nutné dodržovat tyto zásady:

a) zásada koordinace činností,
b) zásada jednotného velení,
c) zásada jednotného postupu,
d) zásada dvojí kontroly,
e) zásada svědomitosti a pečlivosti.

Při dodržení výše uvedených zásad je možno hovořit o dodržení takových opatření, které budou mít za cíl vyhledání a identifikaci veškerých elektronických a digitálních zařízení, které mohou být přítomny na místě činu, a které mohou přispět k objasnění trestní věci.

5.2 Zajišťování digitálních stop

Tato fáze celého procesu zajišťování digitálních stop na místě činu přichází v okamžiku, kdy jsou vyhledány a identifikovány veškeré digitální stopy, které se na místě činu nacházejí, a které jsou označeny jako stopy zájmové pro potřeby dalšího vyšetřování.

Při přípravě k zajištění objektů je nutné:

a) **Zjistit veškeré dostupné údaje o předmětných prostředcích digitální techniky –** zde je myšleno zjištění údajů o typu zařízení, jejich počtu, rozmístění, potřebné kapacitě datového prostoru, napojení na kominikační prostředky, použitý operační systém, apod.,
b) **Zhodnotit situaci a prostředky, které je možno k zajištění objektů zkoumání použít –** tzn. připravit nezbytné technické vybavení,
c) **V případě potřeby vytvořit podmínky pro utajení přípravných prací i samotného samotného úkonu zajištění digitálních stop,**

Při zajišťování digitálních stop a ostatních objektů zkoumání je nutné:

a) **Dodržet včasnost zajišťovacích úkonů** – tzn. dodržet zásadu, že časová prodleva mezi dobou, kdy byla pravděpodobná trestná činnost spáchána a dobou zajištění digitálních stop by měla být taková, aby došlo k co možná nejmenším ztrátám zájmových dat, která by mohla být při nedodržení této zásady smazána, nebo přepsána.
b) **Dodržet rychlost a koordinovanost zajišťovacích úkonů** – tato zásada vyplývá ze skutečnosti, že některé typy výpočetní techniky mohou provádět operace vedoucí ke zničení nebo znehodnocení stop zcela autonomně, bez zásahu lidské činnosti.
c) **Dokumentovat veškeré zajišťovací úkony** – toto je prováděno zejména v případě, že jsou zajišťovány prostředky digitální techniky při nestandardní či neobvyklé konfiguraci, případně, kdy je důležité zadokumentovat zapojení jednotlivých částí zkoumaného zařízení tak, aby bylo umožněno jeho následné zkoumání. Takovouto dokumentaci lze provádět nejen fotograficky, ale lze pořídit i videodokumentaci či topologickou dokumentaci (plánek, náčrtek).
d) **Brát v úvahu výskyt jiných upotřebitelných stop** – v tomto případě je vhodné posoudit, zda ze zajištěného zařízení nebude možné získat např. stopy daktyloskopické či genetické, které by byly využitelné pro zkoumání.

Zabezpečení zajištěných dat a techniky:

a) **Při zajišťování dat je nutné zabezpečit jejich integritu –** data jsou opatřena kontrolním součtem a celý postup zajišťovacích prací je dokumentován,
b) **Při zajišťování techniky vyloučit její záměnu, neoprávněný přístup a manipulaci –** toho je docíleno přijetím takových opatření, kdy je technika ihned po provedení fotodokumentace uložena do předem připravených transportních obalů. Současně je nutno zabránit poškození zajištěné techniky mechanickými a fyzikálními vlivy.

5.3 Vytváření záloh a bitových kopií digitálních stop

Technologický postup zavedení operačního systému GNU/Linux do zájmového počítače a následné vytvoření bitové kopie disku je složen z několika na sebe navazujících kroků, které musí být bez výhrady dodrženy. Níže uvedený postup vytvoření bitové kopie je pouze jednou z mnoha možností, jak bitovou kopii na místě činu pořídit. V této práci bude uveden postup, kde je využíváno práce v systémovém terminálu. Samozřejmě, že existují i varianty, které umožňují pro vytvoření bitové kopie využít některou s utilit, která je nabízena (např. nástroj Guymager nebo G-parted). Tyto utility mají svou nespornou výhodu v tom, že uživatel pracuje v grafickém prostředí, a tudíž odpadá složitější práce se systémovým terminálem a ručním zadáváním jednotlivých příkazů. Z mého pohledu ovšem patří ovládání systémového terminálu k základům, které by měl každý forenzní IT specialista ovládat. Využívání "klikacích" utilit pro vytváření bitových kopií a pro další forenzní práci na místě činu však nelze jednoznačně nedoporučit – jejich použití může být v určitých situacích výhodou, zejména v okamžiku, kdy forenzní specialista pracuje na rušném místě a pod tlakem. V tento okamžik může být použití grafického rozhraní vnímáno jako benefit, jelikož je snížena možnost vzniku chyby či selhání lidského faktoru v důsledku stresu. Stále však nepřestává platit, že práce v systémovém terminálu je základní dovedností každého forenzního IT secialisty.

5.3.1.1 Vytvoření bitové kopie pomocí operačního systému GNU/Linux:

1. Naformátovat technologický disk na požadovaný souborový systém (nejčastěji NTFS, FAT32, EXT3),
2. Ujistit se, že bootovací sekvence technologického počítače je nastavena na bootovaní z CD/DVD disku, případně USB (volba záleží na tom, z jakého média chceme zavádět operační systém),
3. Připojit technologický a zkoumaný disk k počítači, vložit bootovací médium,
4. Po nabootování systému spustit Terminál (příkazová řádka),
5. Zadat příkaz „*sudo su*“ (toto není ve všech distribucích stejné, někdy je vyžadováno pouze zadání samotného „*sudo*“, či „*su*“) pro získání oprávnění roota (administrátorská práva),
6. Příkazem „cat/proc/partitions“ provést vypsání připojených zařízení. Z výpisu je možno identifikovat jak technologický disk, tak i zájmové médium. Pokud by bylo nejasnosti, s identifikací jednotlivých médií, je možno si pomoci zadáním příkazu „lsblk“, což je jedna z dalších variant, jak provést výpis připojených zařízení. Tento příkaz, resp. Jeho výstup, je doplněn o grafické znázornění připojených zařízení a k nim náležejícím oddílům.
7. Technologické médium (ve výpisu identifikováno jako */dev/sdb*) je připojeno k souborovému systému technologického počítače. Toto se provede zadáním příkazu „*mkdir/mnt/techno*“. Tímto příkazem jsme docílili vytvoření tzv. přípojného bodu, ke kterému následně „přimountujeme“ technologický disk. Zájmové médium budiž označeno jako „*/dev/sda*“.
8. Technologický disk se připojí zadáním příkazu „*mount/dev/sdb /mnt/techno*“ Tímto příkazem je deklarováno, že dojde k připojení média „*/dev/sdb*“ do přípojného bodu v adresáři „*/mnt/techno*“, který byl v předchozím kroku vytvořen.
9. Na technologickém disku je doporučeno vytvořit si jednotlivé pracovní adresáře, do kterých budou následně kopírovány bitové kopie či zájmové soubory. Vytvoření pracovních adresářů je možno provést také v systémovém terminálu za pomoci příkazu „*mkdir*“ případně využít postupu, který je dle mého názoru nejen rychlejší a efektivnější, ale také přehlednější. Zadáním jednoduchého příkazu „*mc*“ se spustí Midnight Commander, což je utilita graficky velmi podobná známému souborovému manažeru Total Commander – pomocí této utility velmi podobně jako za pomoci programu TC je možno vytvořit jednotlivé pracovní adresáře. Midnight Commander

se ukončuje klávesou F10. (pozn. utilitu Midnigt Commander neobsahují všechny dostupné distribuce systému GNU/Linux, proto je nutné tento program dodatečně stáhnout z některého z dostupných repozitářů pomocí příkazu: „*sudo apt-get install mc*“). Na závěr řekněme, že byl vytvořen pracovní adresář s názvem „*/mnt/techno/stopa1*“.

10. Zadáním příkazu „*fdisk –lu /dev/sda > /mnt/techno/stopa1/fdisk.txt“* jsou získány informace o struktuře zájmového média je jeho rozdělení na jednotlivé oddíly. Výsledky jsou uloženy do souboru „*fdisk.txt*“ v cílovém adresáři.
11. Dále je nezbytné získat informace o parametrech zkoumaného média. Toto je provedeno zadáním „*hdparm –i /dev/sda > /mnt/techno/stopa1/hdp.txt“*. Tímto příkazem získáme veškeré informace o technicko-výrobních parametrech média, ale i o jeho teplotě, počtu hodin od spuštění, vadných sektorech, apod.
12. Poslední příkaz, ktrerý slouží k získání technických informací o zkoumaném médiu je příkaz „*smartctl –a /dev/sda > /mnt/techno/stopa1/smart.txt“.*
13. Předposledním krokem je samotné zadání příkazu pro vytvoření bitové kopie zájmového média. Nějčastěji se ve forenzní praxi je možno setkat s příkazem „*dd*“, jehož jednoduchá syntaxe zní „*dd if=/dev/sda of=/dev/sdb*“. Tento příkaz byl pro potřeby forenzních činností rozšířen o několik dalších parametrů, které budou dále v textu vysvětleny. Použijeme tedy „*dd if=/dev/sda conv=noerror,notrunc,nosync | md5tee /mnt/techno/stopa1/md5.txt | split –b 700m - /mnt/techno/stopa1/hdd_“*. Samotná struktura příkazu je velmi podobná základní variantě příkazu „*dd*“, zde ovšem do příkazu přidáváme další pokyny, které mají být provedeny v průběhu vytváření bitové kopie. Výsledná bitová kopie je použitím „*split –b 700m*“ dělena do bloků, které mají velikost 700MB. Dále je v průběhu vytváření bitové kopie za poci příkazu „*md5tee*“ počítána kontrolní suma MD5 a ukládána v cílovém adresáři do souboru s názvem „md5.txt“
14. Po ukončení práce je doporučeno zadáním příkazu „*init0*“ technologický stroj vypnout.

Závěrem tohoto technologického postupu je třeba uvést, že existuje mnoho dalších způsobů, jak docílit stejného výsledku, a záleží jen na osobních preferencích každého uživatele, který postup zvolí. Pokud se však uživatel rozhodne používat tento postup, či zvolí jinou, své osobě bližší variantu, nelze toto pokládat za chybu.

Ve forenzní praxi se lze setkat i s dalšími mutacemi příkazu „*dd*“, jejichž použití má také své opodstatnění. Níže uvádím dvě varianty, které jsou pro vytváření bitových kopií používány.

Příkaz „*dc3dd*“:

„*dc3dd if=/dev/sda of=/mnt/techno/stopa1/hdd_ conv=noerror,notrunc,sync progress=on sizeprobe=on hash=md5 hashwindow=700m split=700m splitformat=aa log=/mnt/techno/stopa1/hddlog.txt*“

Příkaz „*dcfldd*“:

„*dcfldd if=/dev/sda conv=noerror,notrunc,sync errlog=/mnt/harddisk/evidence/log.txt hash=md5 hashconv=after hashlog=/mnt/techno/stopa1/hash.txt status=on sizeprobe=if split=700m splitformat=aa of=/mnt/techno/stopa1/hdd_*“

5.3.1.2 Vytvoření bitové kopie na spuštěném systému

Pro potřeby vytvoření bitové kopie na spuštěném systému a zajištění obsahu operační paměti je možno použít celou řadu komerčně i volně poskytovaného softwaru. Mezi nejběžněji používané nástroje je možno zařadit Acces Data FTK Imager, což je velmi oblíbený forenzní nástroj určený pro počítače s operačním systémem Microsoft Windows a GNU/Linux. Dalším, velmi vydařeným řešením je použití forenzního softwaru BlackLight, jenž je specializován na zařízení s operačním systémem Mac OS.

Při práci se spuštěným počítačem je doporučeno postupovat dle níže uvedených bodů:

1. Provede se deaktivace spouštění spořiče obrazovky, režimu spánku či režimu hybernace. Co nejdříve je nutné zjistit, jaká pravidla bezpečnostní politiky jsou pro daný počítač nastavena.
2. Zhodnotí se stav počítače ve vztahu k možnosti připojení externího paměťového média (technologické disky jsou nejčastěji připojovány prostřednictvím USB-SATA redukce).
3. Na technologický disk se nakopíruje forenzní nástroj, kterým bude pořízena bitová kopie a zajištěn obsah RAM paměti. Následně se technologický disk pomocí USB redukce připojí ke zkoumanému počítači.
4. Na připojeném technologickém disku je vyhledána a spuštěna forenzní aplikace.
5. Provede se záloha operační paměti zkoumaného počítače. V případě mnou preferovaného softwaru FTK Imager je volba pro zajištění paměti v menu označena

jako „Capture Memory“ – po stisknutí této volby je následně vybrán cílový adresář, kam bude záloha uložena.

6. Dále je v menu aplikace zvolena volba „Create Disk Image“. Po výběru této volby je po uživateli požadováno vybrat „zdroj“ dat – v tomto případě se může jednat o fyzický disk, logickou jednotku nebo adresář.
7. Po zvolení zdrojové cesty je zvolena cesta cílová, tedy ta, kam budou zálohy v podobě bitové kopie ukládány. Jako cílový adresář je zvolen adresář nacházející se na technologickém disku.
8. Společně s bitovou kopií je do cílového adresáře umístěn také „log“ soubor ve formátu .txt, který v sobě obsahuje spočtenou kontrolní sumu vytvořené bitové kopie. Výpočet konkrétního typu kontrolní sumy není v programu defaultně nastaven, a proto je zde uživateli ponechána možnost si před začátkem vytváření bitové kopie zvolit, který typ kontrolního součtu je požadován.

Po ukončení vytváření bitové kopie je důležité zkontrolovat její funkčnost a převážně úplnost, a to načtením do některého z forenzních programů (EnCase, X-Ways, BlackLight, apod.). V případě, že vytvořená bitová kopie není čitelná, nebo je poškozená, je možno celý postup opakovat. V případě, že by opakování postupu nebylo úspěšné, provede se pouhé vykopírování zájmových souborů na technologický disk.

5.4 Dokumentace, balení a ukládání digitálních stop

Jedná se o poslední fázi činností, které jsou prováděny na místě činu při zajišťování digitální techniky a digitálních stop. I zde je nutné dodržovat nezbytné zásady pro balení a ukládání techniky tak, aby nedošlo k její záměně, neoprávněnému přístupu či manipulaci se zajištěnou technikou.

Balení zajišťované digitální techniky a stop:

a) **Počítače se zpravidla nezajišťují s připojenými periferiemi –** ke zkoumání znaleckému pracovišti jsou počítače ve většině případů zasílány bez připojených periferií. Nelze však vyloučit, že bude nutné zajistit zařízení takového charakteru, kde připojené periferie budou pro průběh zkoumání žádoucí,
b) **Počítače jsou zpravidla zajišťovány v původních krabicích, papírových nebo igelitových pytlích,**

c) **Paměťová média jsou balena jednotlivě (pevné disky počítačů) nebo po skupinách (USB flashdisky, diskety, CD/DVD),**
d) **Pevné disky počítačů jsou baleny do obalů s pěnovou nebo bublinkovou vložkou,**
e) **Diskety, disky ZIP, LS-120, apod. jsou baleny do obalů, které minimalizují vlivy elektromagnetického pole,**
f) **Obaly s optickými disky nesmí umožnit přístup UV záření a musí minimalizovat dopad IR záření na přepravovaná optická média,**
g) **Komunikační a mobilní technika je balena do obalů s pěnovou nebo bublinkovou vložkou, a zároveň je tato technika zabezpečena proti náhodnému stisku klávesnice nebo disleje,**
h) **Plastové karty s magnetickým proužkem jsou baleny do obalů, které minimalizijí vlivy elektromagnetického záření.**

Skladování a přeprava objektů zkoumání:

a) **Zajištěné objekty co nejdříve předat znaleckému pracovišti –** toto by mělo být dodrženo převážně, jedná-li se o zajištěnou mobilní a komunikační techniku, která byla zajištěna v zapnutém stavu,
b) **Zajištěné objekty zabezpečit proti mechanickému počkození a proti počkození způsobenému fyzikálními vlivy –** toto opatření má za cíl minimalizovat dopady mechanických rázů, působení vysokých teplot, vody a vlhkosti či prachu a agresivních látek na zajištěnou digitální techniku,
c) **Paměťová média chránit před slunečním zářením –** jedná se především o média, která jsou založena na principu optického nebo magnetooptického záznamu,
d) **Paměťová média chránit před elektromagnetickým polem –** jedná se především o magnetická a magnetooptická média, která by měla být přepravována ve speciálních obalech tak, aby nebyla ani na krátký okamžik vystavena silnému magnetickému poli. Přepravu takovýchto objektů se nedoporučuje provádět v elektromobilech, či prostředcích hromadné dopravy osob, které jsou poháněny elektrickým proudem.
e) **Objekty zkoumání skladovat v suchém, bezprašném a chemicky neagresivním prostředí,**

f) **Přístroje, které jsou napájeny z dočasných zdrojů energie ihned dopravit na příslušné znalecké pracoviště –** jedná se o přístroje, které jsou napajeny pomocí akumulátorů. V případě, že není možné tyto předměty převést na příslušné znalecké pracoviště, je nezbytné zabezpečit jejich napájení z odpovídajícího přívodu elektrické energie.

g) **Nevysušovat techniku, která byla zajištěna ve vodě –** takovouto techniku (záměrně utopený mobilní telefon) je nutné dopravit na znalecké pracoviště ve vhodném obalu a ponořené ve vodní lázni tak, aby bylo zamezeno oxidaci kovových částí jednotlivých dílů, která by byla způsobena přístupem vzduchu.

Dodržením výše uvedených postupů a doporučení by mělo být zaručeno, že dojde ke správnému a úplnému zajištění všech zájmových objektů, a zároveň budou splněna veškerá kritéria, která budou rozhodující pro aplikaci následných postupů forenzního zkoumání. Jedině za dodržení všech pravidel pro zajišťování digitálních stop může být zaručeno, že budou ke znaleckému zkoumání stopy předány v takovém stavu, který povede k jejich maximální využitelnosti pro potřeby objasňování trestné činnosti.

ZÁVĚR

Rostoucí význam výpočetní a digitální techniky a její pronikání do života každého jedince úzce souvisí i s rostoucím zastoupením počtu elektronických zařízení, která mohou být, nebo jsou využívána k páchání různých forem trestné činnosti. Tento fenomén dělá z počítačů, mobilních telefonů, tabletů a jiných digitálních zařízení žádaný zdroj informací nejen o osobě samotného pachatele, ale i o průběhu protispolečenské události, která se stala, nebo se mohla stát, a která nesla znaky trestné činnosti.

Obsahem této diplomové práce bylo zmapovat a objasnit problematiku digitálních stop, které se nacházejí na místě činu, a které mohou být využitelné pro potřeby vyšetřování orgánů činných v trestním řízení. Teoretická část práce je věnována legislativním aspektům souvisejícím se zajišťováním digitálních stop na místě činu a dále popisuje digitální stopy z hlediska jejich charakteristických vlastností. Cílem práce bylo, mimo jiné, specifikovat, jaké metody jsou uplatnitelné pro zajišťování digitálních stop a popsat možné způsoby, jakými lze vytvořit bitovou kopii zajištěné digitální stopy. Těmto dvěma bodům zadání je v práci věnována samostatná kapitola, ve které jsou specifikovány nejen vhodné metody pro zajišťování stop, ale je zde i popsáno, jakými způsoby lze vytvářet bitové kopie zajištěných digitálních stop.

Stěžejní kapitoly této práce se poté nacházejí v její praktické části, kde je věnován prostor zhodnocení rizik, která mohou nastat při zajišťování digitálních stop. Formulovaná rizika jsou okomentována a u každého z hrozících rizik je navženo protiopatření, které by mělo vzniku daného zábránit. V další samostatné kapitole jsou rozebrány jednotlivé metody, které lze využít při zajišťování digitálních dat, a dále jsou zde formuluvána kritéria, která by měla být rozhodující pro volbu dané metody. Stanovená kritéria byla následně konfrontována s jednotlivými metodami pro zajišťování dat, tak aby bylo zřejmé, jakou z metod zajišťování digitálních stop a za jakých podmínek lze využít na místě činu, aby byl celý proces prací s digitálními stopami technologicky korektní.

Na základě kvalifikovaného odhadu byla definována množina zařízení, reprezentující různorodé typy digitálních stop, které se mohou nacházet na místě činu. U každého jednotlivého zařízení byl proveden návrh metody pro jeho korektní zajištění tak, aby odpovídal stanoveným kritériím a požadavkům na technologickou správnost a také požadavkům na maximální využitelnost stopy v procesu jejího dalšího zkoumání.

V poslední kapitole této diplomové práce byl na základě výše uvedených zjištění navržen obecný technologický postup, který lze aplikovat na jednotlivé druhy digitálních stop, běžně se vyskytujících na místě činu. Cílem tohoto návrhu je přinést jednotný postup, jehož aplikací budou snížena rizika jež byla formulována v jedné z kapitol praktické části práce. Současně by za dodržení všech podmínek tohoto doporučeného postupu měla být zvolena a aplikována taková metoda pro zajišťování stop, která bude za dané situace a okolností nejvíce vhodná, a která povede ke zvýšení využitelnosti stop pro objasnění dané trestní věci.

S postupným rozvojem digitální techniky a nezastavujícím se vývojem nových technologií lze předpokládat jejich rostoucí význam v životě každého jedince. Nelze se však domnívat, že veškerá digitální zařízení budou používána pouze v souladu s dobrými úmysly, pro které byla původně stvořena.

SEZNAM POUŽITÉ LITERATURY

[1] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 9788073805470.

[2] *Trestní zákoník a trestní řád: průvodce trestněprávními předpisy a judikaturou*. Praha: Linde, 2010. ISBN 9788072018086.

[3] KOLOUCH, Jan. *Cybercrime*. Praha: Edice CZ.NIC, 2016. ISBN 978-80-88168-18-8.

[4] VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů*. Zlín, 2013. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[5] KOTHÁNEK, Jaroslav. Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení. *Policie ČR*. Praha, 2008.

[6] NELSON, Bill. *Guide to computer forensics and investigations: processing digital evidence*. 5th edition. ISBN 9781285060033.

[7] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet*. 3rd ed. Waltham, MA: Academic Press, c2011. ISBN 0123742684.

[8] PORADA, Viktor. *Kriminalistika: (teorie, metody, metodologie)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. ISBN 9788073804909.

[9] KONRÁD, Zdeněk a Jiří STRAUS. *Kriminalistika: teorie, metodologie a metody kriminalistické techniky*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. ISBN 9788073805357.

[10] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 9788073805890.

[11] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 9788073805012.

[12] BRADÁČ, Albert, Miroslav KLEDUS a Pavel KREJČÍŘ. *Soudní znalectví*. Brno: Akademické nakladatelství CERM, 2010. ISBN 9788072047048.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Access point – přístupový bod k síti Wi-Fi
FAT	File Alocation Table
IDE	Označení počítačové sběrnice
MD5	Message digest alghorytm
NAS	Network Attached Storage
NTFS	New Technology File System
PC	Personal computer
RAID	Redundant Aray of Independent Disks – vícenásobné diskové pole
RAM	Random Access Memory
SATA	Seriál ATA
SHA-1	Secure Hash Alghorytm -
SHA-2	Secure Hash Alghorytm
SAS	Seriál Attached SCSI
OS	Operační systém
SIM	Subscriber Identity Module
USB	Universal Seriál Bus
Wi-Fi	Wireless Fidelity

SEZNAM OBRÁZKŮ

SEZNAM TABULEK